Approche unifiée défaillance-dommage dans la sûreté de fonctionnement pour la régénération des matériels au combat : application aux systèmes d'armes terrestres

Maxime Monnin

N° d'ordre : 09-07

Thèse

PRÉSENTÉE À
L'UNIVERSITÉ DE VALENCIENNES ET DU HAINAUT CAMBRÉSIS

en vue de l'obtention du titre de

DOCTEUR de l'Université de Valenciennes

Spécialité Automatique Industrielle et Humaine

Par

Maxime MONNIN

Approche unifiée défaillance/dommage dans la sûreté de fonctionnement pour la régénération des matériels au combat
Application aux systèmes d'armes terrestres

Soutenue le 10 Octobre 2007 devant la Commission d'examen composée de :

D. NOYES	**Rapporteur**	Professeur à l'Ecole Nationale d'Ingénieurs de Tarbes
N. REZG	**Rapporteur**	Professeur à l'Université Paul Verlaine de Metz
P.E. LABEAU	**Examinateur**	Professeur à l'Université Libre de Bruxelles
Y. DUTUIT	**Examinateur**	Professeur à l'Université Bordeaux 1
C. TAHON	**Examinateur**	Professeur à l'Université de Valenciennes
O. SÉNÉCHAL	**Co-Directeur**	Professeur à l'Université de Valenciennes
B. IUNG	**Co-Directeur**	Professeur à l'Université Henri Poincaré Nancy I
P. LELAN	**Invité**	Délégation Générale pour l'Armement
M. GARRIVET	**Invité**	Société NEXTER Systems

LAMIH - UMR CNRS 8530 - UVHC

N° d'ordre : 09-07

Thèse

PRÉSENTÉE À
L'UNIVERSITÉ DE VALENCIENNES ET DU HAINAUT CAMBRÉSIS

en vue de l'obtention du titre de

DOCTEUR de l'Université de Valenciennes

Spécialité Automatique Industrielle et Humaine

Par

Maxime MONNIN

Approche unifiée défaillance/dommage dans la sûreté de fonctionnement pour la régénération des matériels au combat
Application aux systèmes d'armes terrestres

Soutenue le 10 Octobre 2007 devant la Commission d'examen composée de :

D. NOYES	**Rapporteur**	Professeur à l'Ecole Nationale d'Ingénieurs de Tarbes
N. REZG	**Rapporteur**	Professeur à l'Université Paul Verlaine de Metz
P.E. LABEAU	**Examinateur**	Professeur à l'Université Libre de Bruxelles
Y. DUTUIT	**Examinateur**	Professeur à l'Université Bordeaux 1
C. TAHON	**Examinateur**	Professeur à l'Université de Valenciennes
O. SÉNÉCHAL	**Co-Directeur**	Professeur à l'Université de Valenciennes
B. IUNG	**Co-Directeur**	Professeur à l'Université Henri Poincaré Nancy I
P. LELAN	**Invité**	Délégation Générale pour l'Armement
M. GARRIVET	**Invité**	Société NEXTER Systems

LAMIH - UMR CNRS 8530 - UVHC

A ma fille Romane, sa soeur Léa et leur maman Audrey,

A mes parents

Remerciements

Mes remerciements s'adressent tout d'abord, à Benoît Iung, Professeur à l'Université Henri Poincaré et Olivier Sénéchal, Professeur à l'Université de Valenciennes, pour toute la confiance qu'ils m'ont accordée. Leurs précieux conseils ainsi que leur disponibilité m'ont permis de mené à bien ces travaux et d'acquérir les bases d'une démarche scientifique.

Je remercie vivement Monsieur Daniel Noyes, Professeur à l'ENI de Tarbes et Monsieur Nidhal Rezg, Professeur à l'Université Paul Verlaine de Metz d'avoir accepté d'être les rapporteurs de ce travail.

Je tiens à remercier également Monsieur Christian Tahon, Professeur à l'Université de Valenciennes ainsi que Monsieur Pierre-Etienne Labeau, Professeur à l'Université Libre de Bruxelles qui ont accepté d'examiner les travaux présentés dans ce mémoire. Je remercie tout particulièrement Monsieur Yves Dutuit, Porfesseur à l'Université de Bordeaux I, pour avoir accepté de présider ce Jury.
Je souhaite également remercier ici Monsieur Michel Garrivet, de la société NEXTER pour sa disponibilité et ces conseils pendant ces trois années, son expérience de la modélisation et de la simulation a été pour moi une grande source de connaissance. Je tiens également à exprimer toute ma gratitude à Monsieur Pascal Lelan, de la Délégation Générale pour l'Armement qui a largement participer à ces travaux en leur donnant une orientation originale. Merci à toutes ces personnes d'avoir d'accepté d'évaluer mon travail en qualité de membre du Jury.

Je souhaite également exprimer toute ma reconnaissance à Eric Levrat, Maître de Conférences à l'Université Henri Poincaré pour nos nombreuses discussions ; merci pour ta patience et tes conseils ...

Merci également à toutes et à tous que j'ai côtoyés pendant ces trois ans, Salah *(le loup - "mon copain de bureau")*, Salah, Zied et Alex, Rémi, David, Ramy, Rony, Pierre, Nico, Cristian, Ed ; une mention toute particulière à William et Sylvaine ! Vous avez tous

largement contribué à notre aventure Nancéenne ...

J'écris "notre aventure Nancéenne" car je termine ces remerciements avec une pensé toute particulière pour ma femme Audrey, merci pour ton soutien sans faille, tu as toujours cru en moi, et toujours su me redonner courage et motivation dans les moments difficiles.

Table des matières

Table des figures

Abréviations et sigles

ACCP	Anti Char Courte Portée
AFIS	Association Française d'Ingénierie Système
AMDEC	Analyse des Modes de Défaillance de leurs Effets et de leur Criticité
AN	Activity Network
BDF	Bloc Diagramme de Fiabilité
BOA	Bulle Opérationnelle Aéroterrestre
CAESAR®	Automoteur de 155 mm/52 calibres entièrement qualifié pour les tirs des charges modulaires.
CDT	Commandement
DDM	Détecteur de Départ Missile
DGA	Délégation Générale pour l'Armement
DoD	Department of Defense
EBRC	Engin Blindé à Roues de Contact
EI	Element Intermédiaire
ELI	Equipe Légère d'Intervention
EM	Elément de Manoeuvre
EMAT	Etat Major de l'Armée de Terre
FMDS	Fiabilité Maintenabilité Disponibilité Sécurité
FTRE	Fault Tree with Repeated Events
IS	Ingénierie Système
MCO	Maintien en Condition Opérationnelle
MIM	Munition Intelligente tirée de Mortier ou de tube de canon
NATO	North Atlantic Treaty Organization
NRBC	Nucléaire Radiologique Biologique Chimique
NTI	Niveau Technique d'Intervention

NTIC	Nouvelles Technologies de l'Information et de la Communication
OBS	Observation
OMG	Object Management Group
RDC	Réparation des Dommages au Combat
RdP	Réseaux de Petri
RdPSG	Réseaux de Petri Stochastiques Généralisés
SAL	Semi-Actif Laser
SAN	Sanitaire
SAN	Stochastic Activity Networks
SC3	Système de Cohérence de Combat de Contact
SdF	Sûreté de Fonctionnement
SdS	Système de Systèmes
SGTIA	Sous-Groupement Tactique Inter-Armes
SIC	Système d'Information et de Communication
SIT	Système d'Information Terminal
SRNs	Stochastic Reward Nets
SSYST	Sous-Système
SysML	System Modeling Language
UML	Unified Modeling Language
VAB	Véhicule de l'Avant Blindé
VBCI	Véhicule Blindé de Combat d'Infanterie
VOA	Véhicule d'Observation d'Artillerie
XL	Char Leclerc
ZU	Zone Urbaine

Introduction Générale

L'évolution des technologies de l'information et de la communication apporte de nouvelles possibilités dans la définition des systèmes d'armes terrestres. L'information revêt un caractère critique dans les phases stratégiques de la manœuvre et conduit à mieux intégrer les moyens d'informations et de communication dans les systèmes d'armes, voire même à faire évoluer la façon dont ceux-ci sont conçus. Ces nouvelles exigences militaires relatives à l'exploitation des capacités technologiques futures a conduit la DGA (Délégation Générale pour l'Armement) à définir le concept de Bulle Opérationnelle Aéroterrestre (BOA). Ainsi, la définition des forces terrestres futures repose sur les trois concepts fondateurs de la BOA : l'info-valorisation, la polyvalence opérationnelle et la synergie des effets. Pour ce faire, l'exploitation dans le combat aéroterrestre de l'ensemble des possibilités offertes par les NTIC (Nouvelles Technologies de l'Information et de la Communication) conduit à accroître les cinq grandes exigences du combat moderne :

- produire les effets justes,
- limiter les phases d'engagement violent, à forte létalité, dans le temps, l'espace et les volumes de moyens engagés,
- accroître la protection des forces,
- maîtriser l'empreinte logistique,
- améliorer la mobilité stratégique et opérative.

Le concept de BOA conduit donc à une rupture dans la façon de concevoir les systèmes d'armes futures et est à l'origine de nombreuses études amont notifiées par la DGA aux principaux industriels de l'armement français : Thales Communication, Sagem DS et NEXTER Systems[1], (L. Barraco 2006). En particulier, la BOA amène à considérer une capacité opérationnelle globale conduisant à la notion de Système de Systèmes (SdS) info-valorisé dont on ne spécifie pas le contenu mais les performances globales. Ces performances globales doivent être déclinées et allouées sur les systèmes futurs (engin blindé médian, missile de combat terrestre...) ou sur les matériels existants à moderniser. Les fonctions du système de combat seront réparties sur les différents systèmes (futurs et existants) et l'information sera partagée par les systèmes qui seront connectés en réseau.

[1]Giat Industries a récemment changé de nom pour devenir NEXTER Systems.
http ://www.nexter.fr/

L'efficacité résultante repose sur la complémentarité des moyens et des unités opérationnelles qui fonctionnent alors en synergie. Les critères de performances doivent donc être appréciés au niveau global. Les performances globales reposent sur l'architecture du SdS et se déclinent sur les fonctions opérationnelles des différentes plates-formes d'une part, et sur l'organisation du soutien logistique pour le maintien en condition opérationnelle (MCO) des plates-formes, d'autre part. Ainsi, les missions, les moyens et l'organisation du soutien logistique sont repensés au sein du concept BOA afin d'optimiser le MCO des systèmes. En effet, le MCO permet de garantir la finalité du SdS par une optimisation de la disponibilité opérationnelle des systèmes qui le composent et constitue par ailleurs la principale composante du coût global de possession. En ce sens, il peut donc être considéré comme un des principaux leviers d'action sur la performance globale du SdS, (A. Muller 2005). Le système de soutien, garant du MCO, devra notamment, (DGA 2005) :

- être à la fois proactif pour soutenir la manœuvre planifiée et réactif pour répondre aux aléas du combat,
- procurer un soutien au plus près du contact par insertion de modules logistiques spécialisés, agiles et protégés, dimensionnés pour permettre prioritairement la survie des blessés, l'accomplissement de l'action planifiée en cours et l'autonomie nécessaire aux actions d'opportunité,
- permettre **une régénération** des systèmes par des capacités à mener facilement des opérations de réparations des dommages subis au combat et/ou des défaillances.

La régénération peut donc être caractérisée par une performance de régénérabilité du SdS qui va dépendre à la fois des possibilités offertes par chaque plate-forme constituant le SdS et par le système de soutien associé. Si les enjeux de la régénération semblent bien identifiés, la définition, la spécification et la maîtrise des performances de régénérabilité des systèmes constituent à ce jour un axe fort dans les études relatives à la BOA. En effet, pour NEXTER Systems notamment qui conçoit et intègre des systèmes d'armes complexes et plus particulièrement des véhicules blindés terrestres, la prise en compte d'exigences de régénération dès la phase de conception des systèmes soulève un ensemble de problématiques.

En effet, la mise en œuvre du concept de régénération au sein d'un SdS dans le contexte BOA, nécessite d'être capable de définir, spécifier et maîtriser cette nouvelle performance à la frontière de la Sûreté de Fonctionnement "classique" et de la survivabilité des systèmes. En effet, la Sûreté de Fonctionnement (SdF) ou "sciences des défaillances" consiste à connaître, évaluer, prévoir, mesurer et maîtriser les défaillances des systèmes au travers d'un ensemble de mesures définissant les performances de Fiabilité, Maintenabilité, Disponibilité et Sécurité des systèmes (FMDS). Dans le processus d'ingénierie des systèmes, ces performances se déclinent en un ensemble d'exigences non-fonctionnelles, et conduisent à la construction de modèles des systèmes pour leur évaluation. Pour ce faire, dans la phase de conception des systèmes, un ensemble d'outils et méthodes sont disponibles pour la construction des modèles supports aux évaluations des performances de SdF. La survivabilité quant à elle, consiste à évaluer les systèmes au regard des menaces (intentionnelles) liées au contexte d'emploi à travers des performances telles que

la vulnérabilité et la susceptibilité. De la même manière, la survivabilité repose sur un ensemble d'outils et méthodes particulier permettant d'appréhender les dommages que subissent les systèmes au combat. Dans ce contexte, NEXTER systems doit donc être capable dès les phases de conception des systèmes d'intégrer les exigences de régénération afin de pouvoir, à la livraison des systèmes, en garantir un degré de régénérabilité au même titre que le taux de disponibilité ; ces deux éléments constituant des arguments commerciaux majeurs. La régénération constitue en ce sens un nouveau challenge dans la définition des systèmes d'armes futurs. Par ailleurs, la DGA doit quant à elle, être en mesure de définir des architectures de système de systèmes qui intègrent des capacités de régénération afin de trouver le meilleur compromis - disponibilité d'une architecture déployée vs. coût de l'architecture - pour une mission donnée. La régénération a de ce point de vue un impact sur la conception des systèmes, d'une part, et sur leur exploitation, d'autre part. Il est donc nécessaire, pour pour répondre aux problématiques posées par la régénération de disposer d'outils et de méthodes permettant d'appréhender conjointement défaillances et dommages afin d'évaluer l'impact de la régénération sur la disponibilité opérationnelle de systèmes, cette évaluation pouvant porter soit sur des solutions de conception particulières, soit sur une exploitation particulière.

En ce sens, notre contribution, développée dans le contexte d'une thèse financée par la DGA, en partenariat avec NEXTER Systems, a pour objet de définir une méthodologie de modélisation des systèmes d'armes basée sur une approche unifiée défaillance/dommage dans la Sûreté de Fonctionnement. Fondée sur l'unification des concepts relatifs à la régénération notre originalité porte tout d'abord sur la proposition d'un modèle de données, structurant les différents éléments nécessaires à l'évaluation de la disponibilité opérationnelle des systèmes en présence de défaillance, de dommage et de régénération. Elle porte ensuite sur la proposition d'un atome générique représentatif du comportement des composants et sur la proposition de mécanismes de construction génériques qui permettent de contraindre la construction des atomes de modélisation dans le respect de la description du système initiée dans le modèle de données. Enfin, les atomes de modélisation sont agrégés pour définir un modèle dynamique qui constitue le support de l'évaluation de la disponibilité opérationnelle du système global. Cette contribution sera développée dans ce mémoire en 4 chapitres.

Tout d'abord, il convient dans un premier chapitre de préciser le concept de BOA au travers des enjeux qu'il représente et, plus particulièrement, au niveau des capacités de sûreté de fonctionnement et de survivabilité visées pour les Systèmes de systèmes qu'il met en oeuvre. Ces performances doivent donc être considérées dès les phases amont de conception dans l'ingénierie des systèmes et soulèvent un ensemble de verrous scientifiques relatifs à l'intégration des dommages et de la régénération dans les méthodes et outils nécessaires pour spécifier et évaluer les solutions de conception au regard des performances de sûreté de fonctionnement et de survivablité.

Cela nous conduit dans le deuxième chapitre à nous intéresser aux travaux scientifiques et industriels qui apportent des solutions en termes de méthodes et d'outils pour

la caractérisation des performances de sûreté de fonctionnement et de survivabilité. Nous verrons comment défaillances et dommages sont appréhendés dans les différents travaux et ce qu'implique la régénération au regard des analyses de disponibilité, de survivabilité et de maintenabilité.

Sur la base des conclusions du précédent chapitre, notre contribution sera développée sur les chapitres III et IV. Le troisième chapitre développe le principe d'unification défaillance/dommage qui constitue la base de notre contribution. Cette unification nous amène, par le biais d'une représentation cohérente des défaillances, des dommages et de la régénération, à proposer un atome de modélisation générique du comportement des composants et des fonctions des systèmes. La deuxième partie du chapitre est consacrée à la formalisation des connaissances nécessaires à la construction des différents atomes de modélisation définissant ainsi un modèle structurel statique correspondant à une description structurée du système. Les règles de construction de ce modèle statique sont formalisées par un ensemble de diagrammes de classes UML définissant ainsi une approche générique indépendante du système modélisé.

Le quatrième chapitre s'appuie sur le modèle structurel précédemment présenté pour définir un ensemble de mécanismes génériques de construction des atomes de modélisation à partir des connaissances formalisées dans le modèle structurel. Ces mécanismes permettent de garantir la cohérence entre les atomes de modélisation développées et la connaissance formalisée dans le modèle structurel pour un système particulier. Ensuite, l'utilisation des Stochastic Activity Networks est justifiée pour porter les atomes de modélisation représentatifs du comportement des systèmes et support aux simulations pour l'évaluation de la disponibilité opérationnelle.

Enfin, le dernier chapitre est consacré à une application de la démarche proposée à un Système de systèmes militaire. Le système de systèmes considéré se caractérise par une architecture (nombre, type de systèmes ainsi que leurs relations) particulière ainsi que par un profil d'emploi. L'objectif de cette expérimentation est, d'une part, de montrer la faisabilité de la méthodologie proposée en développant des modèles sur la base d'un exemple représentatif d'une architecture réelle en terme de taille et de complexité et, d'autre part, d'évaluer l'impact de solutions de régénération sur les performances des systèmes.

Chapitre 1

La régénération des matériels, une nouvelle capacité au coeur de la BOA

Partant des nouvelles capacités attendues du système de combat de contact futur, nous montrons dans ce chapitre quels sont les impacts sur la conception des systèmes dans un contexte d'ingénierie. Les concepts à la base de notre contribution sont présentés ainsi que son objectif principal.

1.1 Introduction

La délégation générale pour l'armement prépare le futur et s'attache à exploiter au mieux les nouvelles technologies au bénéfice de la Défense. Le concept BOA en est une illustration. Son principe repose sur l'action combinée d'un ensemble d'entités (hommes, véhicules robots, drones) qui pourront à la fois communiquer, observer, renseigner et agir en s'appuyant à la fois sur les technologies existantes et sur de nouvelles à développer. La performance globale de l'ensemble repose sur les performances des différentes entités et notamment sur leur disponibilité opérationnelle. Le maintien en condition opérationnelle des plates-formes est donc primordial et a conduit à définir des nouvelles capacités pour le soutien logistique dans le contexte BOA.

1.2 Systèmes de Combat Futurs et Bulle Opérationnelle Aéroterrestre

1.2.1 Le concept de Bulle Opérationnelle Aéroterrestre

Le principe de BOA, bulle opérationnelle aéroterrestre, a été défini par la DGA en liaison étroite avec l'armée de terre (EMAT n.d., DGA 2002, DGA 2005, L. Barraco 2006). Il a été conçu pour répondre aux nouvelles exigences militaires en exploitant les capacités technologiques futures (la miniaturisation par exemple). Ce projet fait suite à la nouvelle démarche de conception des futurs armements français entamée depuis 1997. L'approche traditionnelle par armée ne permettait pas de garantir, dans la durée, toutes les cohérences (opérationnelle, technique, organisationnelle, calendaire) nécessaires à l'efficacité du dispositif militaire. Ainsi, la prospective de défense s'appuie sur une approche par systèmes de forces. BOA s'inscrit dans le système de forces « maîtrise du milieu aéroterrestre ». BOA est constituée autour de véhicules blindés de masse réduite (18-25 tonnes) disposant de leur armement propre (canons, missiles, etc.). Son efficacité repose sur la complémentarité de moyens qui fonctionnent en synergie. Ainsi, par exemple, robots et drones de renseignement et de combat apporteront une capacité d'observation et d'intervention accrue. Celle-ci permet la réponse la mieux adaptée à la menace détectée. Le principe essentiel est basé sur une mise en réseau des capteurs de tous types (imagerie visible ou infrarouge, radars, etc.) et des moyens d'intervention, afin que chacun bénéficie du partage de la situation tactique et en retour participe à son élaboration (compte-rendu de situation par exemple). Plusieurs facteurs sont déterminants pour les interventions aéroterrestres futures :

- amélioration de la protection des combattants,
- développement de la capacité de transport des combattants,
- multiplication des interventions en zones urbaines (au Liban par exemple),
- variété des interventions (de la maîtrise de la violence à la coercition, exemple : Kosovo),
- numérisation du champ de bataille.

Ainsi, les nouvelles caractéristiques des systèmes d'armes terrestres concernent pour les plus remarquables :

- la capacité à combattre un adversaire au plus tôt, parfois au-delà de la vue directe,
- une protection moins individuelle et plus globale (hommes, matériels),
- la mise en place, sur des plates-formes automatisées (drones, robots terrestres) de certaines fonctions à risques importants pour l'homme (exemple : illumination laser de l'objectif afin de guider le tir),
- la capacité à disposer d'une information complète sur la situation opérationnelle, en recoupant des informations provenant de capteurs terrestres (radars), aériens (avions, drones) ou spatiaux (satellites).

Ces nouvelles caractéristiques attendues des systèmes d'arme amènent une rupture dans la façon de concevoir les systèmes et impliquent de revoir complètement l'architecture du combat de contact autour de son système d'information et de gestion du combat introduisant la notion de Système de Systèmes ; la réflexion porte aujourd'hui sur la capacité opérationnelle globale du système de contact aussi, l'efficacité opérationnelle et les critères de performances doivent être appréciés à ce niveau.

De plus, la recomposition du paysage géopolitique et géostratégique de la fin du $20^{ème}$ siècle a modifié à la fois la nature de la menace et son champ d'application. La frontière autrefois claire, entre une menace militaire et une menace qui ne l'était pas, est devenue très floue. C'est aujourd'hui le modèle de société tout entier qui est visé par les acteurs des nouvelles menaces. Le spectre des menaces que doivent prendre en compte les forces terrestres s'est ainsi considérablement élargi. Une même unité pourra avoir à remplir, quasi simultanément, des missions de coercition, de maîtrise de la violence et d'aide aux populations.

L'hostilité de l'environnement pour les matériels et les personnels induit donc à la fois une exposition accrue des systèmes aux dommages, relatifs aux agressions produites par les menaces, et une nécessité de pallier rapidement les défauts de fonctionnement. Il devient donc primordial de garantir la performance globale du système de combat afin de lui permettre d'avoir au bon moment, et pour la durée souhaitée, des personnels compétents disposant des matériels nécessaires et en état de fonctionnement.

La mise en oeuvre de nouvelles technologies pour la mutation des capacités opérationnelles des matériels accroît leur complexité et fait de leur maintien en condition opérationnelle une dimension majeure de leur disponibilité (Cour des comptes 2004).

1.2.2 Le Soutien Logistique : principal acteur du Maintien en condition Opérationnelle

La disponibilité opérationnelle va donc dépendre, d'une part, de la fiabilité et de la maintenabilité du système et, d'autre part, de la réactivité et de l'efficacité de son soutien logistique qui assure le maintien en condition opérationnelle (MCO).
Le maintien en condition opérationnelle nécessite donc la mise en oeuvre d'un ensemble de processus et de moyens (ravitaillement, acquisition et gestion des rechanges, opérations

de maintenance, outillages, documentation, formation,...) nommés éléments du soutien logistique (figure 1.1)[1].

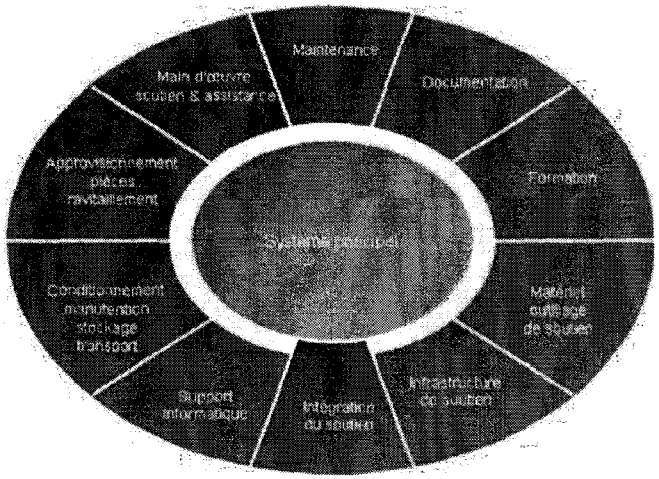

FIG. 1.1 – Les éléments du Soutien Logistique

Aussi, le processus de maintenance considéré comme l'un des principaux leviers d'actions sur la performance globale (O. Sénéchal 2004), constitue le processus clé du MCO au sein des éléments de soutien logistique (A. Muller 2005). Dans les Armées, le processus de maintenance se décline suivant trois niveaux techniques d'intervention (NTI). Un NTI représente un ensemble de moyens en personnels et en matériels permettant de faire face à des charges de maintenance qualitativement et quantitativement définies.
Le NTI 1 assure la mise en oeuvre de la maintenance en ligne du matériel (traitement en piste avant et après vols pour les aéronefs, entretien courant des bâtiments de la marine). Les opérations sont effectuées avec des moyens limités, par les utilisateurs des matériels eux mêmes ou par des structures légères de proximité. Ainsi, par exemple, le NTI 1 des bateaux est assuré par les équipages eux mêmes, parfois en mer. Pour le matériel roulant, ce NTI 1 s'apparente aux opérations qu'un utilisateur de voiture averti peut réaliser lui-même sur son véhicule.
Le NTI 2 correspond aux opérations de maintenance préventive programmée ou curative visant soit à restaurer le potentiel de "vie" des équipements, soit à réaliser des réparations lourdes, exécutées par un organisme de soutien dédié, situé ou non sur le site des utilisateurs. Les équipements nécessaires au NTI 2 sont adaptés à ce niveau d'intervention, plus poussé que le NTI 1.
Le NTI 3 correspond aux opérations "lourdes" de maintenance programmée préventive de reconstitution de potentiel ("grandes visites") ou de réparations à caractère industriel exécutées chez les industriels ou dans des établissements spécialisés nécessitant des moyens véritablement industriels. Ces opérations sont souvent l'occasion de remises à

[1] Association Française d'Ingénierie Système - http ://www.afis.fr

niveau et de modernisation des matériels ou de leurs équipements.

La préparation et l'organisation de la maintenance suivant chacun des NTI, fondées sur les études de fiabilité, maintenabilité et disponibilité, constituent donc l'élément fédérateur de l'analyse des autres éléments de soutien et permettent d'appréhender le maintien en conditions opérationnelles sur l'ensemble du cycle de vie des systèmes avec une considération du soutien dès la conception afin de l'optimiser dans les phases d'exploitation[2].

Soutien Logistique et BOA

Dans le nouveau contexte BOA, la maîtrise de l'empreinte logistique[3] constitue une des cinq exigences que doit satisfaire le système de contact. Pour ce faire, il est nécessaire de limiter les besoins en soutien logistique, d'optimiser les flux logistiques, et de ramener au strict nécessaire la consommation de munitions en optimisant d'une part, les matériels au regard de leur fonction de soutien, et d'autre part, le système de soutien associé. Un ensemble de capacités endogènes et exogènes ont donc été identifiées pour la maîtrise de l'empreinte logistique. Les capacités endogènes correspondent aux performances attendues de la fonction soutien des différentes plates-formes. Les principales étant :

- une fiabilité renforcée (robustesse, simplicité, maîtrise des technologies employées) ;
- une maintenance facilitée (diagnostic intégré, accessibilité des sous-ensembles, utilisation de technologies duales).

Les capacités exogènes, correspondent quant à elles aux performances attendues du système de soutien. Les plus représentatives sont :

- être à la fois proactif pour soutenir la manœuvre planifiée et réactif pour répondre aux aléas du combat ;
- procurer un soutien au plus près du contact par l'insertion de modules logistiques spécialisés.
- permettre une maintenance prédictive, par des aptitudes à anticiper les pannes et les besoins d'échanges de pièces, à effectuer les diagnostics au plus près du contact, à déporter ou reporter les tâches de maintenance les plus complexes.
- assurer une régénération des systèmes par des capacités à mener facilement des opérations de réparations des dommages subis au combat et/ou des défaillances.

Les nouvelles capacités visées pour le soutien logistique contribuent donc directement au MCO des matériels avec, d'une part, une fonction de soutien optimisée pour les plates-formes à travers une fiabilité renforcée et une maintenabilité facilitée auxquelles

[2]A l'echelle du cycle de vie, le coût de maintien en condition opérationnelle s'avère très largement supérieur au coût d'acquisition initial d'un système. Ce coût est donc un facteur significatif dans la décision d'acquisition et sa maîtrise doit être une préoccupation majeure tout au long de la conception du système. - http ://www.afis.fr

[3]La maîtrise de l'empreinte logistique vise à limiter les besoins en soutien logistique (plates-formes allégées), optimiser les flux logistiques (meilleure circulation de l'information logistique), tendre vers le minimum nécessaire de munitions (recours aux munitions intelligentes)

s'ajoutent, d'autre part, un axe fort relatif à la notion de régénération des défaillances et des dommages subis au combat.

Cette dualité système principal (représenté ici par les différentes plates-formes) - système de soutien est à la base du concept de soutien logistique intégré où l'analyse du soutien logistique s'intègre à l'ingénierie du système dès les études amonts (figure 1.2[4]).

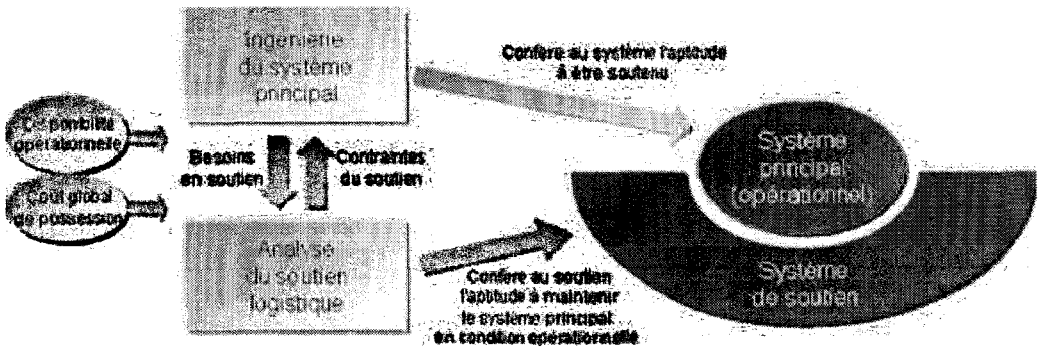

FIG. 1.2 – Approche du soutien logistique intégré

Soutien Logistique Intégré

Le soutien logistique intégré permet donc la cohérence globale de l'ensemble système principal et système de soutien, (DoD 1992, J-P. Meinadier 2002) avec :

- la prise en compte des exigences de soutien dès le début de l'ingénierie système,
- la vérification, tout au long de la conception, de l'aptitude du système à son soutien et de l'aptitude du système de soutien à répondre aux exigences de disponibilité et aux contraintes de maintenance dues aux choix techniques,
- la préparation des acteurs aux tâches d'exploitation, de logistique et de maintenance.

Il participe donc à l'optimisation de la disponibilité opérationnelle des systèmes dans le sens où il permet à chaque étape de la conception de vérifier l'adéquation des capacités du système de soutien avec les caractéristiques de fiabilité et de maintenabilité du système principal.

Ainsi le système de contact futur, défini autour du concept BOA par les capacités nouvelles qu'il nécessite et procure simultanément, impose une approche système telle que définie par l'Ingénierie Système pour la définition d'architecture de système de systèmes offrant les meilleurs compromis au regard du rapport : $\frac{\text{Disponiblité Opérationnelle}}{\text{Coût global de possession}}$.

[4]http ://www.afis.fr

1.3 La disponibilité opérationnelle des systèmes, une performance clé au coeur de l'Ingénierie des Systèmes

L'introduction de la notion de système de systèmes et l'évolution de la nature des expressions du besoin militaire vers une spécification de capacité globale nécessitent d'évoluer dans la façon de définir et spécifier les systèmes. Afin de mieux s'inscrire dans cette évolution, la DGA est membre associé de l'AFIS depuis le 1er Janvier 2007[5].

1.3.1 Introduction à la notion de système de systèmes

Si la définition d'un système est aujourd'hui bien acquise, celle d'un système de systèmes (SdS) est moins évidente et il n'existe pas de définition universellement acceptée (A.P. Sage et C.D. Cuppan 2001). Dans (M. Jamshidi 2005) on trouve notamment 6 définitions relatives aux systèmes de systèmes avec notamment trois définitions se rapportant à des applications militaires (W.H. Manthorpe 1996, R. Pei 2000, A.P. Sage et C.D. Cuppan 2001). Pour sa part, la DGA a retenu la définition énoncée dans (A.P. Sage et C.D. Cuppan 2001) selon laquelle, un système de systèmes est un "système, constitué lui-même de systèmes, et répondant largement aux critères suivants :

- indépendance opérationnelle des sous-systèmes (chaque système constituant dispose d'une consistance opérationnelle à lui seul),
- indépendance managériale des sous-systèmes (chaque système constituant est managé par une entité autonome et sans lien avec un autre constituant, menant chaque système constituant à avoir une ligne de vie indépendante des autres),
- définition et configuration évolutive du système (la définition du système de systèmes est en perpétuelle évolution),
- distribution géographique des sous-systèmes (tous les constituants ne se déplacent pas en bloc),
- comportements émergents du système (certaines fonctions du système de systèmes ne peuvent être attribuées à l'un des systèmes en particulier et ces fonctions perdurent même si l'on perd l'un des constituants du système de systèmes)".

La considération du système de contact comme un système de systèmes fait donc apparaître la notion de comportements émergents, qui sont déterminés, soit dès l'analyse du besoin (auquel cas le SdS est alors conçu pour répondre au besoin), soit par hasard, sur le terrain. Ces comportements émergents s'appuient nécessairement sur les fonctions de chacun des systèmes constituants et par conséquent, la prévision des dégradations des capacités du SdS à l'indisponibilité d'un système constituant est primordiale. La considération de la disponibilité opérationnelle au travers des études de SdF intervient donc dès l'analyse du besoin.

[5]http ://www.afis.fr/nav/orgafis/membres/membres.html

1.3.2 Sûreté de fonctionnement et Ingénierie Système

L'analyse des besoins conduit à la définition d'exigences fonctionnelles traduisant les besoins (ce que doit faire le système) et d'exigences non fonctionnelles traduisant des contraintes imposées au système (performances, qualité de service, environnement). Dans le processus de conception, la sûreté de fonctionnement se traduit donc par un ensemble d'exigences non fonctionnelles et a pour objectif de répondre :

- d'abord aux exigences de fiabilité du système particulièrement contraignantes dans les systèmes critiques (transports, espace, nucléaire,militaire,...) souvent soumis à certification,
- ensuite aux exigences de disponibilité, mettant en jeu des propriétés de fiabilité et de maintenabilité intrinsèques au système, mais aussi d'efficacité de son système de maintien en condition opérationnelle. Elles répondent à des attentes de qualité de service généralement sous-tendues par des impératifs économiques.

Pour ce faire, elle nécessite une approche système (ne pas laisser de maillon faible) qui englobe l'ensemble des activités d'ingénierie système au travers de l'étude structurelle et dynamique des systèmes du point de vue prévisionnel, mais aussi opérationnel en tenant compte des aspects probabilités et conséquences des dysfonctionnements (G. Zwingelstein 1995). La démarche d'obtention de la SdF se déroule donc de l'analyse du besoin à l'intégration en passant par les différents processus de l'ingénierie système comme le montre la figure 1.3[6].

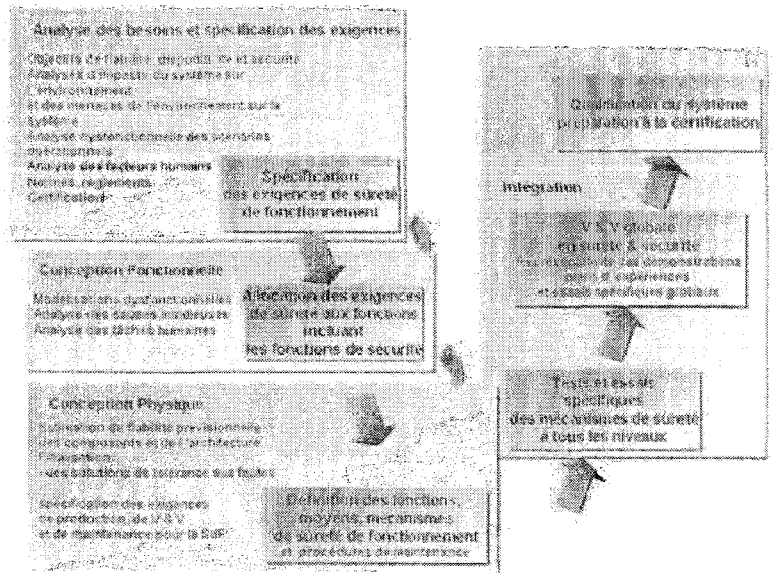

FIG. 1.3 – Schéma de la démarche d'obtention de la sûreté de fonctionnement

[6]http ://www.afis.fr

1.3.3 Les facteurs d'indisponibilité

Pour les systèmes d'arme, les dysfonctionnements d'un système peuvent provenir d'une part du système lui-même en cas de défaillance et d'autre part, d'agressions intentionnelles issues de l'environnement hostile d'exploitation causant des dommages sur le système.

Aussi, la considération des dommages subis par le système d'arme au travers des études de survivabilité constitue une étape incontournable dans l'analyse des dysfonctionnements. La définition de la survivabilité n'est pas unique, nous nous appuierons dans un premier temps sur la définition retenue par la DGA :

Définition 1.1. *Faculté d'un système d'arme à conserver sa capacité opérationnelle entière, partielle ou à uniquement préserver l'équipage face aux menaces représentées par les systèmes d'arme adverses.*

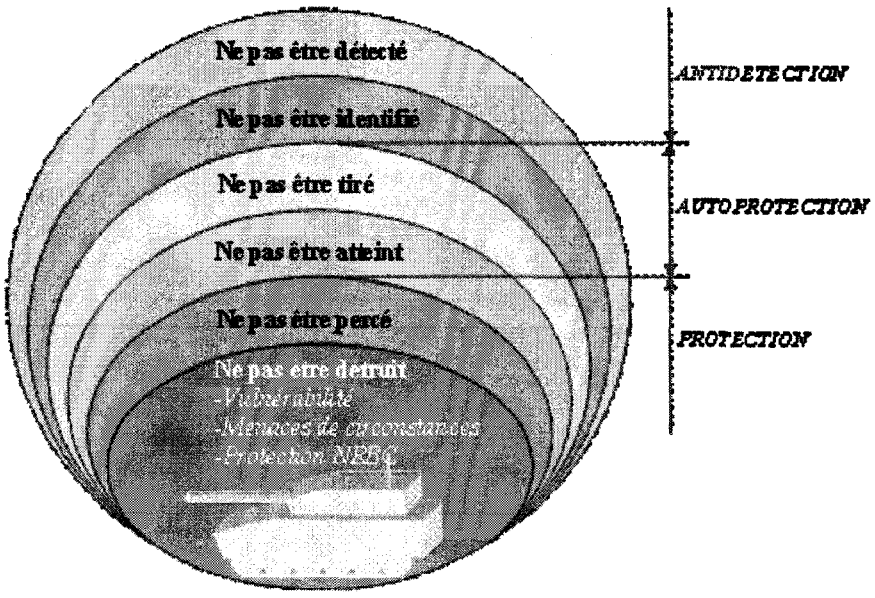

FIG. 1.4 – Principales composantes de survivabilité

La survivabilité s'attache donc à caractériser la vulnérabilité organique et fonctionnelle du système, (figure 1.4), après agression en évaluant les effets sur les occupants du système et les équipements. Nous verrons notamment dans le chapitre III comment cette définition peut être exploitée. Son évaluation dès la conception doit permettre de définir des actions qui interviennent avant et pendant l'agression :

- si possible, éviter les dommages (techniques de furtivité, d'autoprotection)
- au pire les minimiser (Protection balistique, anti-mines... et réduction de la vulnérabilité).

Cependant, la survivabilité qui constitue une caractéristique principale des systèmes d'arme, reste aujourd'hui découplée de la SdF aussi, la régénération des systèmes par le soutien logistique qui nécessite de prendre en compte simultanément défaillance et dommage ce trouve donc à la frontière de la survivabilité et de la SdF. Ce constat a conduit la DGA, par le biais d'une étude prospective technico-opérationnelle à établir un parallèle entre défaillance et dommage pour la prise en compte de la régénération des matériels (J. Perrin, P. Esteve et X. Le Vern 2001b), qui constitue l'idée fondatrice de nos travaux.

1.3.4 Le parallèle défaillance/dommage

La conception de systèmes à disponibilité maximale nécessite de prendre en compte les dommages dans la conception, au même titre que les défaillances techniques. Cette prise en compte est d'autant plus naturelle que les deux notions sont proches, voire interdépendantes :

- proche car, dans un cas comme dans l'autre, il s'agit de prévenir des risques de dysfonctionnement et de mettre en place des solutions permettant de minimiser le temps d'indisponibilité (la figure 1.5 montre le parallèle qui peut être établi entre défaillance et dommage (J. Perrin, P. Esteve et X. Le Vern 2001a)),
- interdépendantes car,
  - d'une part, un dommage peut causer une défaillance et à l'inverse, une défaillance peut être source de dommage,
  - d'autre part, une solution favorisant la maintenance peut avoir un impact sur les possibilités de régénération[7].

La différence fondamentale entre les deux notions est la cause du dysfonctionnement et surtout son mode d'action. Par opposition à la défaillance, le dommage peut être "étendu et aveugle" : le chemin de pénétration et l'impact d'un vecteur d'agression dans un matériel vont impliquer, à des degrés divers, l'ensemble des équipements situés par construction dans la zone concernée, sans relation aucune avec la fonction assurée par ces équipements ; alors que l'origine est facilement identifiable, les conséquences peuvent s'avérer très difficiles à diagnostiquer de manière exhaustive. De plus, les dommages subis au combat étant plus probables que les défaillances, il est nécessaire de compléter la politique de maintenance par une politique de régénération (J. Perrin, P. Esteve et X. Le Vern 2001a), telle que définie par les nouvelles capacités du soutien logistique (cf. §1.2.2). Ainsi, aux exigences de fiabilité (relatives aux défaillances), de vulnérabilité (relatives aux dommages), s'ajoutent donc des exigences de régénérabilité (relatives à l'aptitude du système aux réparations des défaillances et des dommages). Une analyse conjointe des défaillances et des dommages, et ce dès la conception doit donc faciliter la prise en compte de ces exigences de régénérabilité dans le processus d'ingénierie des systèmes.

[7] à titre d'exemple, la protection des pièces critiques limite la vulnérabilité (donc le risque de dommage) mais peut diminuer la maintenabilité

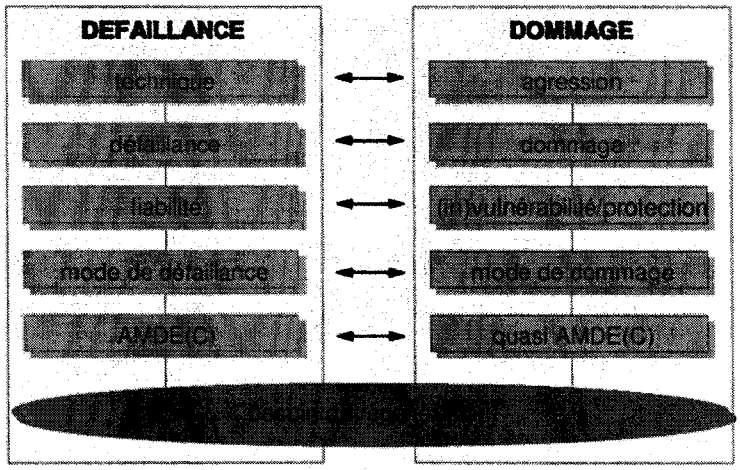

FIG. 1.5 – Parallèle entre la gestion des défaillances et des dommages, (J. Perrin, P. Esteve et X. Le Vern 2001a)

1.4 Vers une Ingénierie de Régénération intégrée à l'Ingénierie Système

En prolongeant le parallèle entre maintenance et régénération, il est possible de définir une ingénierie de régénération à intégrer dans le processus global de l'ingénierie système du programme. Basée sur les études de SdF, l'ingénierie de régénération participe aux différentes phases de l'ingénierie système :

- analyse du besoin : la possibilité de régénérer les matériels doit être prise en compte dans la déclinaison des exigences de disponibilité,
- conception : aux tâches de conception existantes, il faut ajouter une allocation des exigences de régénérabilité des sous-systèmes et équipements
- plans de SdF et de soutien logistique intégré : ils doivent être complétés par une prise en compte des dommages et des études d'analyse du soutien logistique orientées vers la régénération.

Les études de SdF doivent intégrer les analyses de vulnérabilité, et définir des critères de régénérabilité pour pouvoir caractériser les actions de régénération. Les analyses du soutien logistique doivent également intégrer l'analyse des tâches de régénération afin de préciser le concept de régénération par niveau d'intervention et permettre la définition du système de régénération (en complément du système de soutien).

Comme l'ingénierie système (figure 1.6), l'ingénierie de régénération doit s'appuyer sur un ensemble de processus définissant les activités à faire (le :*quoi faire ?*). Ces activités sont réalisées suivant différentes méthodes (*comment ?*), elles même supportées par des outils (*avec quoi faire ?*), éventuellement regroupés en atelier (J-P. Meinadier 2002).

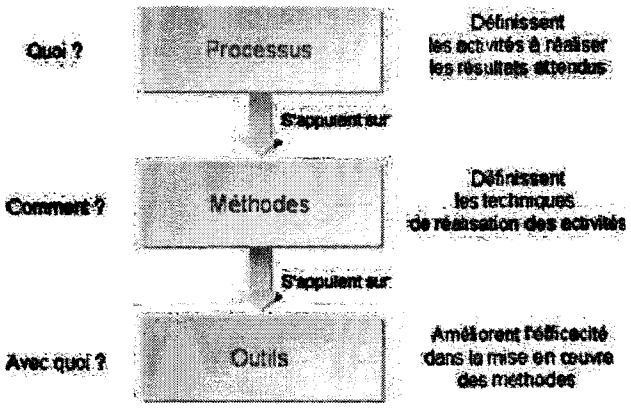

FIG. 1.6 – Rôles respectifs des processus, méthodes et outils

Plus particulièrement, les méthodes recouvrent deux aspects. D'une part, elles sont caractérisées par un aspect *démarche* qui explicite la manière de réaliser les activités des processus en s'appuyant sur des outils assurant la part automatisable de la démarche. D'autre part, elles reposent sur une représentation de tout ou partie du système considéré, par le biais de langages de modélisation. Cette modélisation peut correspondre à différents niveaux d'abstraction selon différents points de vue (fonctionnel, dynamique, structurel, décisionnel) et peut également exploiter des techniques de simulation pour prévoir et valider des comportements, performances et aptitudes du systèmes (J-P. Meinadier 2002). En ce sens, l'ingénierie de régénération doit s'intégrer à l'ingénierie des systèmes au travers d'une approche méthodologique proposant une méthode de modélisation des systèmes permettant de prendre en compte de manière unifiée défaillances, dommages et régénération. Cette méthodologie a pour objectif de fournir une aide à la définition des systèmes de systèmes en permettant l'évaluation de la disponibilité opérationnelle dès les phases de conception, d'une part, et d'évaluer des architectures particulières au regard de profils d'emploi particuliers, d'autre part. De plus, les outils supports de l'ingénierie de régénération devront notamment s'intégrer aux autres ateliers d'ingénierie système. Pour ce faire, il est nécessaire de s'appuyer sur les modèles de données existants, qui assurent la cohérence entre les entités manipulées au cours des travaux d'ingénierie. Participant notamment à la définition des architectures, l'ingénierie de régénération sera basée sur le modèle décrivant les données de haut niveaux manipulées dans le processus de conception d'architectures (GT Modélisation et Outils 2002) présenté à la figure 1.7.

1.5 Conclusion

Si la démarche d'obtention de la SdF est relativement bien éprouvée au sein de l'ingénierie des systèmes (cf figure 1.3), l'introduction du concept de régénération au niveau

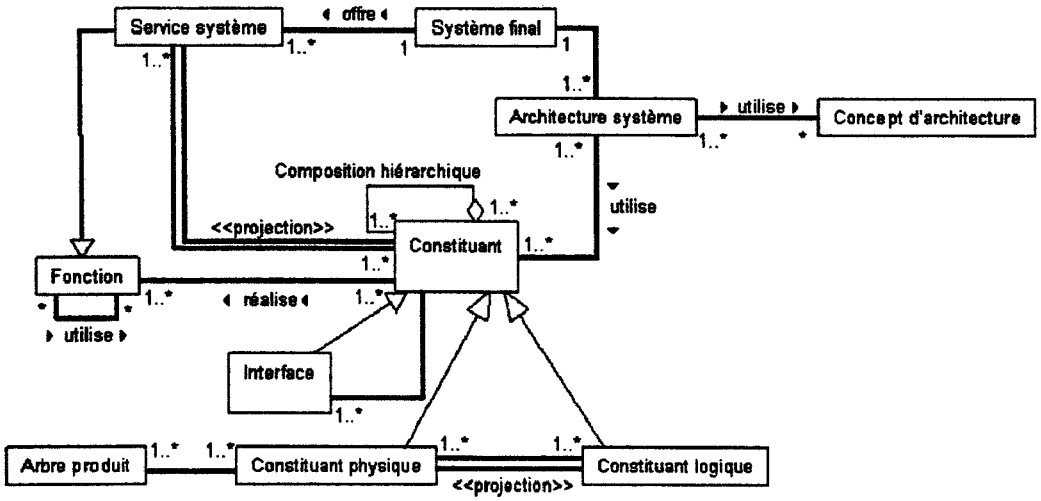

FIG. 1.7 – Modèle de données, Vue Architecture

du système de contact futur soulève encore un ensemble de problématiques. En effet, d'ores et déjà, certains programmes d'armement terrestre incluent des exigences de régénérabilité que les maîtres d'oeuvre industriels vont devoir intégrer dans leur conception (J. Perrin, P. Esteve et X. Le Vern 2001a). Pour ce faire, des éléments sont avancés dans (J. Perrin, P. Esteve et X. Le Vern 2001b) avec notamment la mise en lumière du parallèle existant entre défaillance et dommage (cf. §1.3.4). Sur cette base nous avons montré qu'une ingénierie de régénération peut être définie pour la prise en compte d'exigences de régénérabilité dès la conception des systèmes dans le processus d'Ingénierie Système. Dans ce contexte, notre contribution a pour objectif de formaliser cette ingénierie de régénération à travers une méthodologie de modélisation des systèmes qui permet d'intégrer de manière unifiée défaillances, dommages et régénération pour l'évaluation de la disponibilité opérationnelle des systèmes. Aussi, nous mettons en évidence, dans le chapitre II, les apports et les limites des contributions scientifiques relatives à la modélisation des défaillances, des dommages pour l'évaluation de la disponibilité des systèmes.

Chapitre 2

Modélisation pour l'évaluation de la disponibilité opérationnelle

Dans ce chapitre, nous nous intéressons à l'évaluation de la disponibilité opérationnelle des systèmes et, plus particulièrement, aux méthodes et techniques permettant de développer des modèles de disponibilité opérationnelle.

2.1 Introduction

Dans le processus de conception des systèmes, la SdF regroupe un ensemble de méthodes et d'outils permettant de garantir les exigences de fiabilité et de disponibilité. Comme nous l'avons vu au chapitre premier, les systèmes critiques au regard de l'accomplissement de leur mission et évoluant dans un contexte hostile comme les systèmes militaires doivent intégrer en plus des défaillances, les dommages subis au combat et la régénération dans l'évaluation de la disponibilité opérationnelle. En effet, la régénération caractérise des actions palliatives réalisées après l'occurrence d'une défaillance ou d'un dommage, visant à redonner aux matériels des capacités fonctionnelles leur permettant de terminer leur mission. En ce sens, elle joue un rôle primordiale sur la disponibilité opérationnelle qui dépend à la fois des propriétés de fiabilité (pour les aspects défaillances), de vulnérabilité (pour les aspects dommages) et de maintenabilité (pour la régénération) des systèmes. Les modèles nécessaires à l'évaluation des performances de SdF et, plus particulièrement, de la disponibilité opérationnelle doivent donc permettre de formaliser en un tout cohérent des connaissances sur :

- les défaillances techniques et leurs mécanismes de propagation (point de vue fonctionnel),
- les dommages subis au combat (impact physique) nécessairement liés à la mission (impact du contexte opérationnel),
- la régénération des défaillances et des dommages matérialisée par un retour à un état fonctionnel (impact fonctionnel et du contexte opérationnel).

Dans ce chapitre, nous aborderons donc tout d'abord comment les méthodes et outils de la SdF sont utilisés dans le contexte d'Ingénierie Système pour répondre aux nouvelles exigences de disponibilité opérationnelle et quelles sont leurs limites au regard de la considération des défaillances, des dommages et de la régénération. De la même manière, nous montrerons ensuite comment les travaux traitant de la survivabilité des systèmes contribuent à la caractérisation de la disponibilité opérationnelle et dans quelle mesure ils répondent à la problématique de régénération. Enfin, une synthèse permettra de conclure quant aux verrous scientifiques restant à lever pour contribuer à l'ingénierie de régénération pour l'évaluation de la disponibilité opérationnelle.

2.2 Sûreté de Fonctionnement et Disponibilité Opérationnelle

2.2.1 Concepts et définitions

D'une manière générale, la SdF peut être considérée comme une performance caractéristique des systèmes de systèmes. Elle se décline en quatre grandeurs quantifiables que sont : la Fiabilité, la Maintenabilité, la Disponibilité et la Sécurité (FMDS). L'obtention des performances de SdF d'un système passe par la mise en oeuvre d'une *démarche de SdF* qui vise à évaluer ces grandeurs caractéristiques. En ce sens, la SdF regroupe un ensemble de méthodes et d'outils supports à l'évaluation des grandeurs FMDS. On parle

alors des méthodes et outils de la SdF[1]. Enfin, la SdF peut également correspondre à un ensemble d'objectifs tels que :

- la prévision des dysfonctionnements,
- la tolérance aux défauts et aux pannes,
- les démonstrations d'obtention de la sûreté.

Chacun de ces objectifs peut donc être évalué en terme de grandeurs FMDS par le biais de méthodes et outils de la SdF (e.g. la fiabilité d'un système évaluée à partir de la construction d'arbres de défaillances peut caractériser sa tolérance aux défauts et aux pannes). La SdF revient donc à rechercher et exploiter a priori les informations relatives aux événements redoutés : pannes, agressions, aléas..., à les prendre en compte pour des décisions plus fines, plus justes, dans la définition des systèmes. En ce sens, elle fournit les éléments pour évaluer le risque pris en fonction des choix d'architecture, de politique de maintenance, etc. La SdF dépend donc nécessairement de la connaissance disponible sur le système étudié (Yves Mortureux 2001). Cette démarche ou raisonnement "sûreté de fonctionnement" repose sur des notions de base (principalement la fiabilité, la maintenabilité, la disponibilité) que nous allons préciser ici par un ensemble de définitions. L'ensemble des définitions est tiré de la norme (AFNOR 2001).

Définition 2.1. ***La fiabilité***

Aptitude d'une entité à accomplir les fonctions requises dans des conditions données pendant une durée donnée.

La mesure de la fiabilité permet donc d'évaluer la capacité d'un système, d'un sous-système ou d'une entité E à maintenir une fonction dans des conditions données continûment dans le temps. Elle est caractérisée par la probabilité $R(t)$ (R comme Reliability) dont l'expression mathématique associée est :

$$R(t)=Probabilité\ (E\ non\ défaillant\ sur\ [0,t])^2$$

La fiabilité est souvent exprimée en fonction du taux de défaillance instantané $\lambda(t)$ représentant l'intensité de défaillance en fonction du temps. L'expression de la fiabilité $R(t)$ devient alors à :

$$R(t) = exp(-\int_0^t \lambda(u).du) \tag{2.1}$$

Généralement l'hypothèse est souvent faite que le taux de défaillance est constant. La loi de fiabilité prend alors la forme suivante :

$$R(t) = exp(-\lambda.t) \tag{2.2}$$

[1]Par exemple la méthode AMDEC (Analyse des Modes de Défaillance de leurs Effets et de leur Criticité a pour objectif d'identifier les modes de défaillance d'un système et de les caractériser en termes de cause, conséquences et criticité. Cette méthode constitue une étape à l'obtention des grandeurs FMDS et est considérée comme une méthode de la SdF

[2]$R(t)$ est une fonction non croissante variant de 1 à 0 sur $[0, +\infty[$

Définition 2.2. ***La maintenabilité***

Aptitude d'une entité à être remise en état d'accomplir des fonctions requises dans les conditions données, par une maintenance donnée.

La maintenabilité traduit l'aptitude d'un matériel à être remis en état de fonctionnement et se caractérise par la probabilité $M(t)$. $M(t)$ est la probabilité pour que le système soit réparé sur l'intervalle [0, t], sachant qu'il est défaillant à l'instant t=0. L'expression correspondante est donc :

$$M(t)=Probabilité\ (E\ réparé\ sur\ [0,t])^3$$

Comme la fiabilité, la maintenabilité peut être exprimée en fonction du taux de réparation instantané $\mu(t)$, la maintenabilité s'écrit alors :

$$M(t) = 1 - exp(-\int_0^t \mu(u).du) \tag{2.3}$$

Comme pour la fiabilité, si μ est supposé constant on obtient :

$$M(t) = 1 - exp(-\mu.t) \tag{2.4}$$

La notion de maintenabilité nécessite d'expliciter les moyens (procédures, outils, organisations...) mis en oeuvre pour remettre l'entité en état d'assurer son service. De ce fait, ce n'est a priori pas une grandeur intrinsèque à l'entité. Mais, à conditions d'utilisation données, à moyens de maintenance fixés, c'est une caractéristique de l'entité. La disponibilité qui dépend de la fiabilité et de la maintenabilité est définit comme suit :

Définition 2.3. ***La disponibilité***

Aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée.

Elle correspond donc à la proportion de temps passé en état de remplir les fonctions requises dans des conditions données. Elle se caractérise par la probabilité $A(t)$ d'être non défaillant à l'instant t :

$$A(t)=Probabilité\ (E\ non\ défaillant\ à\ t)$$

Dans le cas de systèmes non réparables, l'étude de la disponibilité se ramène à l'étude de fiabilité et $A(t) = R(t)$.

[3] $M(t)$ est une fonction non décroissante variant de 0 à 1 sur $[0, +\infty[$

Autres grandeurs

De ces grandeurs fondamentales peuvent être déduites des estimations de durées liées aux événements de défaillance et de réparation d'une entité. Les plus couramment utilisées sont :

- le MTTF (Mean Time To Failure) : durée moyenne de bon fonctionnement avant la première défaillance,
- le MTTR (Mean Time To Repair) : durée moyenne de réparation,
- le MDT (Mean Down Time) : durée moyenne de l'état défaillant,
- le MUT (Mean Up Time) : durée moyenne de bon fonctionnement,
- MTBF (Mean Time Between Failure) : durée moyenne entre deux défaillances.

La disponibilité opérationnelle peut alors être définie comme le rapport : $\frac{MUT}{MUT+MDT}$, dans lequel le MDT prend en compte tous les facteurs d'indisponibilité (délai administratif, délai logistique, etc)

Les démarches et les moyens de la Sûreté de Fonctionnement

Pour évaluer les grandeurs de la SdF, de nombreuses méthodes et démarches ont été développées, leur objectif étant de fournir un cadre structuré pour représenter qualitativement et/ou quantitativement les défaillances. Elles sont principalement de deux types, (C. Betous-Almeida 2002) :

- *ordinales* : elles sont alors destinées à identifier, classer et ordonner les défaillances ou les méthodes et techniques pour les éviter,
- *probabilistes* : elles permettent alors d'évaluer en termes de probabilités le degré de satisfaction de certains attributs de la SdF.

Les méthodes et techniques destinées à effectuer les deux types d'analyses peuvent être spécifiques comme, par exemple, l'AMDEC pour l'évaluation ordinale, ou les chaînes de Markov pour l'évaluation probabiliste, ou alors utilisées dans les deux formes d'évaluation : diagrammes de fiabilité, arbres de défaillances par exemple. Face à la complexité croissante des systèmes, les méthodes probabilistes permettent à la fois de considérer des phénomènes réellement aléatoires et d'appréhender de manière pertinente des phénomènes complexes mal connus. Dans les approches probabilistes, on trouve principalement les modèles combinatoires et les modèles états-transitions. L'évaluation de la disponibilité opérationnelle qui nécessite la considération de comportements de type défaillance/réparation s'appuie sur les modèles états-transitions au pouvoir de modélisation plus étendu, plus à même de représenter des comportements complexes (J. Muppala, R. Fricks et K. Trivedi 2000). Ainsi, pour prévoir et valider les comportements des systèmes au regard des performances de SdF, des modèles sont développés pour permettre de reproduire le comportement du système. Dans la typologie des modèles utilisés en ingénierie système (figure 2.1), les modèles de SdF correspondent aux modèles analytiques dont le traitement fournit une évaluation numérique des performances de SdF. De manière générale, le processus de modélisation à la base de l'évaluation des performances de SdF se décompose en trois phases :

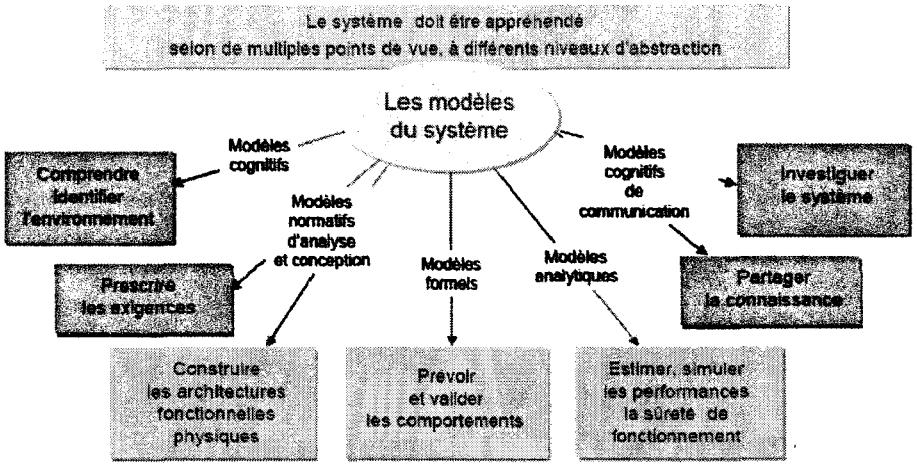

FIG. 2.1 – Typologie des modèles pour l'Ingénierie Systèmes - http ://www.afis.fr

- choix des *mesures de SdF* à évaluer, qui fait généralement partie de l'expression des besoins du système étudié (cf.figure 2.1),
- *construction du modèle*, ou modélisation, qui décrit le comportement du système étudié à partir des processus stochastiques élémentaires et en fonction des mesures considérées,
- *traitement du modèle*, qui correspond au calcul des grandeurs de SdF.

Nous nous intéressons plus particulièrement en ce qui concerne les mesures de SdF, aux modèles de disponibilité opérationnelle qui permettent de rendre compte à la fois de la fiabilité et de la maintenabilité des systèmes.

2.2.2 Les modèles états-transitions pour l'évaluation de disponibilité

Les modèles états-transitions appartiennent aux formalismes au pouvoir de modélisation étendu. Ils sont basés sur l'énumération complète des états possibles et des transitions entre ces états, ils permettent a priori de décrire tous les systèmes à espace d'états discrets. Dans la mesure où le nombre d'états est fini, ils peuvent être représentés par des graphes où les sommets correspondent aux états du système et où les arcs représentent les transitions, (J-F Ereau 1997).

Développées initialement pour construire des modèles de fiabilité, de nombreuses techniques de modélisation permettent de représenter le comportement des systèmes dans le formalisme états-transitions, (K.S. Trivedi et M. Malhotra 1993). Nous ne donnerons pas ici un inventaire complet de toutes les techniques existantes mais nous aborderons des contributions particulières reflétant les principaux atouts de ces techniques de modélisation pour l'évaluation de la disponibilité opérationnelle. Nous analyserons plus particulièrement dans quelle mesure elles permettent de répondre à la problématique d'évaluation de la disponibilité opérationnelle en présence de défaillance, de dommage

et de régénération, sur la base des principaux critères suivants : évaluation de processus stochastiques (approches analytiques, approches par simulation), modélisation des dépendances (grands systèmes complexes), prise en compte de facteurs extérieurs (modélisation des agressions), difficulté d'élaboration des modèles (méthode de construction des modèles).

Les approches analytiques

Classiquement, les modèles de disponibilité reposent sur l'utilisation des chaînes de Markov et des réseaux de Petri (RdP), (M. Malhotra et K. Trivedi 1995) et des méthodes de modélisation ont été développées dans de nombreux domaines d'application tels que : les systèmes informatiques (M. Malhotra et K. Trivedi 1995, C. Betous-Almeida et K. Kanoun 2004b, K. Trivedi et al. 2006), les réseaux de télécommunications (H. Wang et H. Pham 1997, E. Zio, L. Podofillini et V. Zille 2006), l'industrie manufacturière (D.V. Raje et al. 2000, M. Boiteau et al. 2006) ou encore les systèmes militaires (Y. Macheret, P. Koehn et D. Sparrow 2005, K. Upadhya et N. Srinivasan 2003). Le principe à la base de toutes ces techniques indépendamment du formalisme choisi consiste à énumérer les états de bon et de mauvais fonctionnement et de représenter les délais aléatoires de passage d'un état à un autre.
L'utilisation des chaînes de Markov impose cependant des hypothèses particulières quant aux processus stochastiques représentés : ils doivent être représentés par une loi exponentiel à taux constants. Ainsi, dans la plupart des cas ces hypothèses restrictives sont respectées afin de bénéficier de la puissance de modélisation des chaînes de Markov, notamment en terme de dépendances au sein du système à modéliser (J. Muppala et K. Trivedi 1995). L'intérêt de l'approche Markovienne réside dans la possibilité de traiter les modèles de manière analytique, autorisant ainsi un calcul exact des grandeurs de SdF. Cependant des aspects importants du comportement des systèmes dans des modèles de SdF ne peuvent être traités par un modèle Markovien (paramètres non constants, distribution non-exponentielle), et le modèle est alors considéré comme *non-markovien.* Plusieurs approches ont été développées pour traiter les modèles non-markoviens, les principales étant :

- la méthode des variables complémentaires,
- la méthode des états fictifs (ou méthode "phase type"),
- la théorie de renouvellement de Markov.

Toutes ces méthodes ont pour but "d'arranger" le processus non-markovien de manière à ce qu'il devienne analytiquement solvable. Nous invitons le lecteur à se reporter à (J. Muppala, R. Fricks et K. Trivedi 2000) pour plus de précisions sur ces différentes approches.
Il existe cependant plusieurs limitations aux modèles Markoviens. Tout d'abord, étant basés sur l'énumération possible des états du système, de tels modèles posent le problème d'explosion combinatoire du modèle. En effet, un modèle de N composants pouvant prendre chacun deux états compte 2^N états soit plus d'un million d'états pour seulement 20 composants. D'autre part, quand la modélisation nécessite la prise en compte de comportements complexes, la construction de la chaîne de Markov peut vite devenir

fastidieuse et source d'erreurs. Une autre limitation particulièrement restrictive dans notre cas (systèmes sujets aux défaillances avec des taux de défaillance de l'ordre de 10^{-6} (en h^{-1}) d'une part et aux agressions dont l'occurrence est quasi certaine à l'échelle d'une mission (environ 24 h) tient aux difficultés de résolution de tels processus dont les taux de transitions diffèrent de plusieurs ordres de grandeurs. Ces processus qualifiés de Stiff Markov Chains on fait l'objet d'études particulières (A. Bobbio et KS Trivedi 1986, A. Reibman et K. Trivedi 1988) mais induisent une difficulté supplémentaire dans leur résolution.

Une solution aux problèmes de l'explosion combinatoire et de construction du modèle peut être apportée par l'utilisation des RdP. En effet, les RdP stochastiques et, plus particulièrement, les *RdP stochastiques généralisés* (RdPSG) introduits par Ajmone-Marsan, (M.A. Marsan, G. Balbo et G. Conte 1984) offrent une approche graphique pour la modélisation du comportement des systèmes. Une extension particulière aux RdPSG, les *Stochastic Reward Nets* (SRNs), introduite par Cardio *et al.* (G. Ciardo, J.K. Muppala et K.S. Trivedi 1992) offre des possibilités de modélisation encore plus étendues et constitue un formalisme de représentation plus compact que les RdPSG. Malhotra et Trivedi, (M. Malhotra et K. Trivedi 1995) donnent notamment plusieurs exemples de représentations équivalentes entre des RdPSG et des SRNs pour des modèles de fiabilité et de disponibilité. Les SRNs offrent notamment la possibilité de réduire la taille du réseau par rapport au RdPSG équivalent en exprimant différents aspects du système qui seraient explicitement représentés par des places et des transitions dans le RdPSG, par le biais d'expressions arithmétiques ou logiques du taux de récompenses dans le SRN.

D'autre part, un intérêt majeur de l'utilisation des réseaux de Petri stochastiques et de leurs extensions réside dans leur équivalence aux modèles Markoviens. En effet, chaînes de Markov et RdP sont équivalents dans le sens où, dans le cas de modèles Markoviens, la chaîne de Markov équivalente au graphe d'accessibilité des marquages du RdP peut toujours être obtenue. Les liens et les méthodes de passage d'une représentation à une autre ont été établis par Malhotra et Trivedi (M. Malhotra et KS Trivedi 1994) et sont illustrés par la figure 2.2,(J. Muppala, R. Fricks et K. Trivedi 2000).

Enfin, une autre extension des RdP les *Stochastic Activity Networks* (SANs) a été introduite par Meyer, Movaghar et Sanders (J.F. Meyer, A. Movaghar et W.H. Sanders 1985). Ce formalisme a été développé de le but de faciliter la construction de modèles pour l'évaluation de performances et de SdF des systèmes informatiques (W. Sanders 1988). Plus puissants que les RdP, les SANs sont également basés sur une représentation des états par des places, des transitions par des activités (équivalentes aux transitions des RdP) mais ils intègrent en plus la notion de *portes* utilisées pour spécifier le comportement par défaut des activités (W.H. Sanders et J.F. Meyer 2001), offrant ainsi un pouvoir de modélisation supplémentaire par rapport aux RdP. Il existe deux types de *portes* : les *input gates* (liées à l'entrée d'une activité) et les *output gates* (liées à la sortie de l'activité). Les *input gates* autorisent la spécification de conditions particulières pour permettre à l'activité d'être tirée alors que les *output gates* spécifient les fonctions de changement d'états personnalisées qui sont exécutées quand l'activité est tirée. Ainsi, les SANs permettent de considérer des comportements stochastiques détaillés, autorisant la prise en compte de dépendances et d'interactions complexes dans les processus de

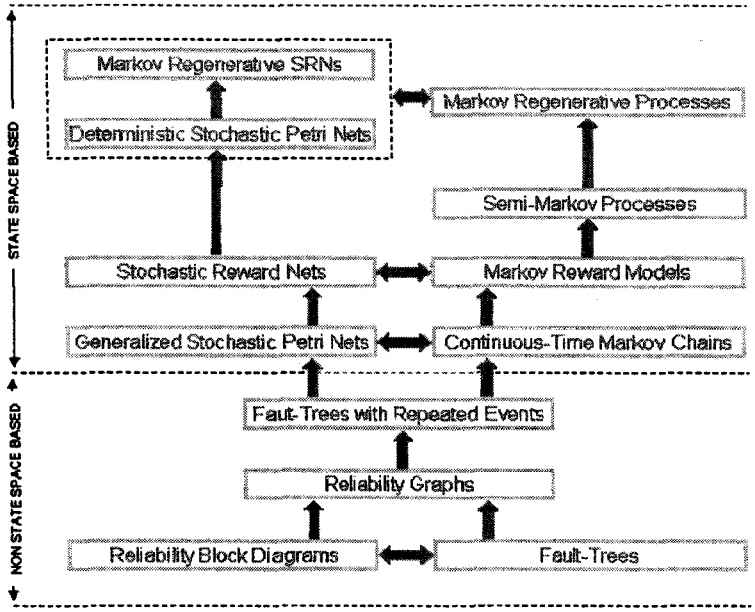

FIG. 2.2 – Equivalence entre les techniques de modélisation, (J. Muppala, R. Fricks et K. Trivedi 2000)

défaillances/réparations. L'utilisation de variables de récompense permet d'obtenir des grandeurs de SdF complexes comme la disponibilité partielle (impact de la perte de composants particuliers sur la disponibilité du système global). Enfin, les SANs supportent soit la résolution analytique du modèle quand la chaîne de Markov équivalente peut être générée (tout comme les RdPSG et les SRNs), soit la résolution par simulations de Monte Carlo, dans le cas de processus stochastiques non markoviens.
Cependant, toutes ces techniques de modélisation souffrent de limitations dans le cas de grands systèmes complexes ne respectant pas l'hypothèse Markovienne. Le traitement analytique n'est plus possible et il est nécessaire de construire des modèles simulables. En effet, la simulation permet de s'affranchir de l'hypothèse Markovienne et offre la possibilité de représenter des comportements complexes, plus proches de la réalité des systèmes.

Les approches par simulation

Pour pallier les restrictions de l'approche Markovienne, d'une part, et le problème de l'explosion combinatoire, d'autre part, de nombreuses approches par simulation de Monte Carlo de l'évaluation de la disponibilité ont été développées, (H. Wang et H. Pham 1997, P.E. Labeau et E. Zio 2002, A.C. Marquez, A. Heguedas et B. Iung 2005). Des approches particulièrement intéressantes couplent l'utilisation d'une représentation

états-transitions du système et des simulations de Monte Carlo pour l'évaluation de la SdF. Ces méthodes bénéficient ainsi de la description graphique des modèles offerte par les formalismes états-transitions et de la puissance de résolution des simulations. Le comportement du système est alors représenté par les états que peut prendre le système et les différentes transitions possibles entre ces états. Les transitions sont régies par des processus stochastiques ou déterministes et les simulations de Monte Carlo permettent de faire évoluer le modèle sur un horizon temporel donné. Chaque réalisation est appelée histoire, on réalise alors N histoires pour obtenir des statistiques sur les grandeurs mesurées. Les modèles sont donc plus proches des caractéristiques des systèmes réels dans le sens où ils intègrent des dépendances complexes entre les composants, des processus stochastiques non-exponentiellement distribués et ils permettent de modéliser des systèmes de grande taille. Parmi les modèles états-transitions utilisés on trouve notamment, les automates (E. Zio, L. Podofillini et V. Zille 2006), les RdP (A. Hein et KK Goswami 1996, J-F Ereau 1997, Y. Dutuit et al. 1997, J.L. Chabot, Y. Dutuit et A. Rauzy 2001), les Stochastic Activity Networks (S.T. Beaudet, T. Courtney et W. Sanders 2006) ainsi que les diagrammes états-transitions (K. Upadhya et N. Srinivasan 2003, K. Upadhya et N. Srinivasan 2004, K. Upadhya et N. Srinivasan 2005). Ainsi, ces méthodes au pouvoir de modélisation étendu permettent de considérer de manière fine de réelles contraintes industrielles et sont particulièrement intéressantes pour des cas d'applications réelles, non académiques.

2.2.3 Synthèse

La palette de méthodes disponibles pour l'évaluation de la disponibilité opérationnelle dans le contexte de la SdF semble être relativement fournie. Cependant, la majeure partie de ces méthodes se focalise sur la considération des défaillances et de leur réparation (remise des composants dans un état nominal). Si les mécanismes de défaillances considérés et les processus de réparation diffèrent d'un champ applicatif à un autre, très peu de contributions font état de facteurs extérieurs venant entraver les performances de SdF. La partie suivante de ce chapitre est donc consacrée à la prise en compte de facteurs extérieurs dans le contexte des études de SdF afin d'évaluer dans quelle mesure il est possible de considérer l'impact des facteurs extérieurs sur la disponibilité opérationnelle.

2.3 Disponibilité et facteurs extérieurs

Globalement, si les modèles classiques sont efficaces au regard des problématiques d'évaluation de la disponibilité opérationnelle, ils correspondent à une vision réduite de la SdF dans le sens où seules les défaillances sont considérées et la maintenabilité est toujours vue comme une caractéristique intrinsèque des systèmes qui ne dépend ni du contexte opérationnel, ni de la nature des défaillances. En effet, en ce qui concerne les événements initiateurs (les causes), la SdF, par définition (c.f. § 2.2.1) ne se limite pas aux défaillances mais peut permettre de prendre en compte aussi bien des agressions de

l'environnement, des actions inattendues ou interdites des utilisateurs ou des tiers, ou d'autres phénomènes aléatoires.

2.3.1 Fiabilité et facteurs extérieurs

En SdF, les facteurs extérieurs sont le plus souvent traités relativement au concept de défaillance de cause commune, (RESS 1991, M. Marseguerra, E. Padovani et E. Zio 1999). Cependant, comme le soulignent Levitin et Lisnianski, (G. Levitin et A. Lisnianski 2003), ces approches considèrent la fiabilité relativement à une formulation de redondance du type *k out of n* et s'attachent à évaluer l'impact de facteurs extérieurs sur la fiabilité de l'ensemble. En ce sens, si les facteurs extérieurs peuvent affecter plusieurs composants en même temps, ces composants participent toujours à la même fonction (composants en redondance). Ces approches ne permettent donc pas de considérer les dommages et leurs mécanismes de propagations. En effet, selon Perrin *et. al*, (J. Perrin, P. Esteve et X. Le Vern 2001a) la considération des dommages dans les études de SdF implique de pouvoir rendre compte de la notion de *dommages aveugles et étendus*, selon laquelle une agression peut affecter simultanément plusieurs composants sans liens fonctionnels.

Si la prise en compte des agressions intentionnelles, que peut subir un système, concerne a priori plutôt les systèmes militaires elle devrait toutefois être permise dans toute démarche de SdF. Cependant les travaux traitant de SdF classique et intégrant des agressions sont rares et la contribution la plus significative revient à Upadhya et Srinivasan (K. Upadhya et N. Srinivasan 2003, K. Upadhya et N. Srinivasan 2004, K. Upadhya et N. Srinivasan 2005). Les auteurs s'intéressent à la modélisation d'une flotte d'avions militaires pour l'évaluation de la disponibilité opérationnelle. Les systèmes (avions et hélicoptères) sont d'abord modélisés par un diagramme états transitions reflétant chaque état possible des systèmes. La considération des dommages que peuvent subir les systèmes les conduit à intégrer un "nouvel état" au regard des modèles présentés précédemment puisque les systèmes peuvent être détruits. En revanche, pour les agressions ne conduisant pas à la destruction des systèmes, les auteurs considèrent que le dommage résultant de l'agression conduit à la défaillance du système. Les agressions sont modélisées par des distributions de probabilités discrètes. Par ailleurs, le contexte opérationnel joue un rôle important dans l'évaluation de la disponibilité à travers la prise en compte de délais logistiques fonctions des missions assignées aux systèmes. En revanche, si la maintenabilité des systèmes n'est pas nécessairement exponentiellement distribuée, la nature de la défaillance (défaillance intrinsèque ou défaillance suite à un dommage) ne modifie pas la maintenabilité. En d'autre termes, la maintenabilité des différents composants des systèmes ne dépend que de leurs dispositions constitutives. Une défaillance survenue après une agression, qui aura nécessairement un impact physique sur le système, ne modifie pas la maintenabilité.

Enfin, compte tenu de la nature non-markovienne du modèle, des simulations de Monte Carlo sont réalisées pour obtenir une évaluation statistique de la disponibilité opérationnelle des systèmes.

De par sa modélisation des agressions et des dommages, cette approche lève plusieurs points relatifs à l'évaluation de la disponibilité opérationnelle en présence de défaillances, de dommages et de régénération. Cependant, la considération d'un processus de maintenance classique, qui ne différencie pas défaillances et dommages, est relativement réductrice. En effet, si les défaillances intrinsèques peuvent être considérées uniquement au regard de leur impact fonctionnel, les dommages résultant des agressions ont nécessairement un impact physique sur le système, (DoD 1980) qui ne peut se réduire uniquement soit à la destruction, soit à la défaillance. En ce sens, leur impact sur la maintenabilité ne peut être négligé.

La considération de facteurs extérieurs dans les disciplines classiques de la SdF, et notamment dans les études de fiabilité, est donc relativement faible et ne rend pas réellement compte des problématiques inhérentes aux facteurs extérieurs : impacts simultanés de plusieurs composants, détériorations physiques des éléments ou encore impact sur les actions de réparations. Ainsi, pour appréhender les facteurs extérieurs ayant un impact sur les performances des systèmes, la concept de survivabilité a été introduit.

2.3.2 Survivabilité

La survivabilité a été introduite il y a une vingtaine d'années dans l'armée de l'air américaine (R.E. Ball 1985). Son objectif principal était d'évaluer la capacité des appareils à éviter ou à résister aux environnements hostiles non naturels. Plus récemment, la notion de survivabilité a été reprise par d'autres domaines d'applications, notamment par le génie informatique (S. Liew et K. Lu 1994, John Knight et Kevin Sullivan 2000, P. Pal et al. 2000, A. Keromytis et al. 2003, Arturo Revilla et al. 2003, Y. Liu, B.V. Mendiratta et S.Kishor Trivedi 2004, Yun Liu et Kishor Trivedi 2004, P. Tarvainen 2004), les systèmes navals (A. Papanikolaou et A. Boulougouris 1998, C. Campbell et D. Starbuck 2005, J. Hill et B. Steinberg 2005, T.A. Santos et C.G. Soares 2005, D. LEE et al. 2005) ou encore pour des systèmes d'alimentation d'énergie (G. Levitin et A. Lisinanski 2000, G. Levitin et A. Lisnianski 2003, G. Levitin et al. 2003). En ce sens, la survivabilité est de plus en plus considérée comme une caractéristique importante des systèmes dans de nombreux domaines d'application. En effet, cette nouvelle discipline qui vise à étendre les études de sûreté en considérant des aspects d'agressions et d'attaques sur les systèmes, en plus des défaillances techniques (plus classiques), a fait l'objet de nombreuses publications. Cependant les définitions rencontrées dans la littérature ne permettent pas de statuer de manière claire sur ce nouveau concept. En effet, la nature même de la survivabilité est encore discutée (grandeur probabiliste ou non) et les éléments qui participent à la survivabilité et donc à son évaluation peuvent être très différents voire contradictoires selon les approches. Présentée de manière générale comme une nouvelle composante de la SdF, on ne trouve pas encore de définition unique comme pour la fiabilité ou la disponibilité admise par toutes les communautés. Tarvainen par exemple, (P. Tarvainen 2004) a recensé six définitions uniquement dans le domaine des systèmes d'information. Une définition semble cependant être communément admise, dans la mesure où elle englobe les caractéristiques principales des autres définitions.

Définition 2.4 (survivabilité). *La survivabilité est la capacité d'un système à accomplir sa mission, de façon opportune, en présence d'attaques, de défaillances ou d'accident.*

Ainsi, deux tendances émergent relativement à cette définition. La première rejoint notamment la définition de la survivabilité considérée par la DGA (cf. définition 1.1) qui tend à considérer la survivabilité comme une caractéristique *passive* des systèmes dans le sens où seule la conception du système va lui donner ses performances de survivabilité. Les systèmes vont donc être caractérisés en terme de vulnérabilité et de susceptibilité, la vulnérabilité caractérisant la capacité du système à supporter la menace et la susceptibilité, sa capacité à éviter la menace. En ce sens, les travaux de Levitin *et. al* (G. Levitin et A. Lisinanski 2000, G. Levitin et A. Lisnianski 2003, G. Levitin et al. 2003) proposent une méthode d'optimisation d'architecture d'un système de production d'énergie qui permet de considérer la vulnérabilité et la fiabilité du système afin d'évaluer des compromis de conception entre redondance et protection. Par exemple, la redondance qui permet d'améliorer la fiabilité d'un système ne concourt pas à sa survivabilité dans le sens où, des composants en redondance situés à proximité l'un de l'autre ne vont pas rendre le système moins vulnérable aux attaques (une agression risque d'endommager les deux composants et de faire perdre le bénéfice de la redondance). La survivabilité du système sera donc d'autant meilleure que les composants redondants seront séparés géographiquement. Les auteurs proposent donc d'évaluer la capacité du système à réaliser sa mission en considérant différents états pour le système chacun correspondant à un niveau de performance particulier déterminé par la combinaison des états défaillants ou endommagés des composants du système ce qui reflète ainsi une disponibilité partielle du système.

D'autres approches vont plus loin dans la considération de la survivabilité et prennent en compte des actions réalisées après l'occurrence d'une défaillance ou d'un dommage pour redonner au système des capacités fonctionnelles (A. Keromytis et al. 2003). La survivabilité devient alors *active* dans le sens où des actions sont menées après l'occurrence d'une agression. Cette interprétation de la définition conduit à des approches telle que celle définie par Liu *et. al*, (Y. Liu, B.V. Mendiratta et S.Kishor Trivedi 2004, Yun Liu et Kishor Trivedi 2004), plus à même de conduire à une évaluation de la disponibilité. Basée sur les mêmes techniques de modélisation que les modèles de disponibilité, cette approche permet une utilisation des chaînes de Markov pour évaluer différentes alternatives d'architectures au regard de la survivabilité. La notion de survivabilité est ici justifiée par le fait que les composants peuvent être défaillants en raison de dommages catastrophiques. Cependant, le processus de dommage n'est pas différencié du processus de défaillance et contrairement aux travaux de Levitin ou Upadhya, les conséquences en sont donc les mêmes. Les différentes architectures se caractérisent notamment par la localisation des composants ainsi que les différents types de redondances envisageables (qui impliquent des reconfigurations différentes du système après un dommage ou une défaillance). Un premier modèle : Markov Availability Model correspond à un modèle de disponibilité du système. Il prend en compte les défaillances potentielles du système, les temps de détection, les temps de switch-over, de synchronisation ainsi que les temps de

réparation. Un second modèle : Performance Model est un modèle d'Erlang du système (file d'attente M/M/c) qui décrit le fonctionnement du système. Une caractéristique particulière des "survivable Architectures" évaluée ici est notamment la possibilité de récupérer des capacités de service voire un service total (performances identiques à celle avant la défaillance).

Ainsi, la mise en oeuvre d'actions visant à restaurer les capacités des systèmes après l'occurrence d'une défaillance ou d'un dommage peut conduire à la définition de méthodologie dont l'objectif est d'évaluer la capacité des systèmes à être restaurés, comme le proposent Campbell et Starbuck (C. Campbell et D. Starbuck 2005) dans le contexte des systèmes d'arme navals. Les auteurs introduisent ainsi la notion de "recouvrabilité" des systèmes, définie comme la capacité du système à restaurer un maximum de capacités fonctionnelles. Dans le même temps, un rapport pour le *Department of Defense*, (Army Regulation 2005), traitant du soutien logistique intégré souligne que "la facilité de réparer sur le champ de bataille" constitue un facteur clé de la survivabilité.

Le concept de survivabilité tend donc à introduire une nouvelle composante à la disponibilité à travers la considération forte d'agressions intentionnelles que peuvent subir les systèmes. Elle conduit à de nouvelles approches selon lesquelles fiabilité et vulnérabilité doivent être appréhendées simultanément. En ce sens, la survivabilité doit intervenir dès la conception des systèmes afin de proposer des architectures les moins vulnérables et les plus fiables possibles. La survivabilité peut alors être considérée comme une caractéristique intrinsèque apportant aux systèmes des capacités à gérer les agressions en terme de susceptibilité (éviter la menace) et de vulnérabilité (résister à la menace) (cf. figure 1.4). En parallèle, et plus particulièrement dans le contexte militaire, la survivabilité intègre une composante supplémentaires liée à la maintenabilité visant à rendre compte de la capacité des systèmes à récupérer des capacités fonctionnelles après l'occurrence d'une agression. Il convient donc d'aborder la maintenabilité des systèmes pour évaluer dans quelle mesure, la maintenabilité peut intégrer la notion de dommage en plus des défaillances pour la régénération.

2.3.3 Maintenabilité et facteurs extérieurs

La maintenabilité est un facteur important influant la disponibilité et le coût du cycle de vie des systèmes, dans le sens où elle doit permettre de quantifier l'aptitude des systèmes à être maintenus ou remis en service et donc a un impact direct sur la disponibilité et les coûts de maintenance (U. Dimesh Kumar et al. 2000). L'évaluation de la maintenabilité dans un contexte d'*ingénierie de la maintenabilité* dès la phase de conception doit permettre de mieux maîtriser les caractéristiques des systèmes affectant la maintenance en termes de ressources et d'organisations pour les actions de maintenance corrective et préventive.

Ces deux définitions permettent de mettre en avant les différents facteurs à considérer dans la maintenabilité. Tout d'abord, la maintenabilité est définie comme une "aptitude du bien ou du dispositif" ; cela signifie donc qu'elle correspond à une caractéristique propre aux systèmes. D'autre part, la maintenabilité dépend également de facteurs tels que :

- les conditions d'utilisation,
- les personnels de maintenance et leurs compétences,
- les ressources impliquées dans le maintien du système,
- les procédures à suivre.

Du point de vue du système, la maintenabilité dépend donc de facteurs intrinsèques et extrinsèques au système. Dans, (W. Tarelko 1995), l'auteur considère deux types de caractéristiques pour la maintenabilité : les caractéristiques de conception et l'organisation de la maintenance. De la même manière, dans (M.F. Wani et O.P. Gandhi 1999), les attributs de la maintenabilité sont répartis en trois catégories : conception, personnel et soutien logistique. Les travaux de Zwingmann (X. Zwingmann 2005) sur l'évaluation de la maintenabilité en conception définissent trois types de critères pour la maintenabilité : des critères intrinsèques, des critères extrinsèques et des critères communs. Enfin, dans un ouvrage de l'Institut de sûreté de fonctionnement[4] sur la maintenabilité (P. Blancho et J. Durand 1999), les auteurs définissent la maintenabilité intrinsèque et la maintenabilité extrinsèque, ainsi que les critères qui les caractérisent. Les définitions proposées sont les suivantes :

Définition 2.5 (maintenabilité intrinsèque). *La maintenabilité intrinsèque est l'aptitude d'un bien à être maintenu ou rétabli dans un état dans lequel il peut accomplir une fonction requise, ceci par considération des dispositions constructives intégrées dans le but de faciliter sa maintenance.*

Dans cette définition, la maintenabilité est donc indépendante des lieux d'emploi, des conditions d'utilisation, de l'effectif et des compétences du personnel chargé de la maintenance et de l'organisation mise en place pour assurer la maintenance du bien.

Définition 2.6 (maintenabilité extrinsèque). *La maintenabilité extrinsèque s'intéresse aux conditions d'approche d'un bien dans un environnement donné concernant les tâches à réaliser par l'homme avant dissociation physique du bien ou après association de ses sous-ensembles et avant sa remise en service.*

La maintenabilité globale d'un système dépend donc de différents aspects qui ne sont pas indépendants. Par exemple, si la conception d'un système va déterminer l'accessibilité aux composants (maintenabilité intrinsèque) et définir les opérations de dépose, la performance des différentes opérations nécessaires va dépendre de l'environnement dans lequel elles seront effectuées (maintenabilité extrinsèque).

D'une manière générale, le calcul d'un indice de maintenabilité revient à agréger la valeur de chaque critère de maintenabilité en considérant les relations de dépendance entre les critères. La dépendance peut être soit *hiérarchique* (W. Tarelko 1995, O. Alvarez et A. Possamai 2002, X. Zwingmann 2005), soit *relative* (M.F. Wani et O.P. Gandhi 1999, C-A. Salvila 2005). Cette relation de dépendance se traduit ensuite dans la plupart des cas par un poids affecté aux critères. L'évaluation de la maintenabilité à partir

[4] http ://www.imdr-sdf.asso.fr/v2/extranet/index.php ?

des critères peut éventuellement être basée sur des techniques particulières telles que la logique floue (C-A. Salvila 2005) ou le calcul matriciel (M.F. Wani et O.P. Gandhi 1999), mais la moyenne pondérée reste largement utilisée. Par ailleurs, l'objectif de ces applications étant principalement l'évaluation de solution de conception, plusieurs auteurs (M.F. Wani et O.P. Gandhi 1999, X. Zwingmann 2005) proposent d'introduire un indice de maintenabilité relatif calculé à partir d'un indice "mesuré" et d'un indice dit "idéal", ce qui permet des comparaisons sur une base commune.

L'évaluation de la maintenabilité constitue une problématique d'actualité aujourd'hui encore très largement traitée, cependant la vision duale : *maintenabilité intrinsèque - maintenabilité extrinsèque* conduit à des traitements partiels de son évaluation. En effet, la plupart des travaux se rapportant à la maintenabilité se focalisent sur les critères intrinsèques de la maintenabilité et s'appliquent tous à des évaluations en phase de conception, faisant ainsi abstraction du contexte opérationnel et des facteurs extérieurs. La maintenabilité est alors évaluée dans le but de caractériser des alternatives de conception des systèmes considérés. Les critères de maintenabilité extrinsèques sont toutefois abordés relativement au concept de "supportabilité" (U. Dimesh Kumar et al. 2000), pour l'évaluation du soutien logistique et non du système principal. De plus, peu d'évaluation de la maintenabilité sont faites dans le but de montrer son impact sur la disponibilité alors qu'elle est toujours considérée comme un facteur important voire primordial pour la disponibilité d'un système. Cependant, par définition, la maintenabilité doit rendre compte de l'aptitude d'un système à être maintenu. De plus, indépendamment du contexte opérationnel, la nature de la défaillance à réparer et son influence sur la maintenabilité sont très rarement prises en compte. Ce point particulier devient d'autant plus important quand le contexte opérationnel peut induire des dommages qui ont un impact physique sur les composants et modifient donc nécessairement leur maintenabilité. Ainsi, la manière "pratique" d'aborder la maintenabilité ne couvre pas la notion de facteurs extérieurs (typiquement les agressions) indispensable à l'évaluation de la disponibilité opérationnelle des systèmes d'arme. Enfin, si la définition initiale de la maintenabilité considère la maintenabilité comme une probabilité : $M(t)$ relative au temps de réparation, les évaluations de la maintenabilité qui considèrent ses critères constitutifs ne conduisent pas à une évaluation probabiliste de la maintenabilité.

2.3.4 Synthèse sur la prise en compte des facteurs extérieurs

La prise en compte de facteurs extérieurs dans l'évaluation de la disponibilité opérationnelle reste un problème ouvert et fait l'objet de nombreuses contributions. S'il existe des modèles et des techniques de modélisation éprouvés pour l'évaluation de la disponibilité dans le cadre de la SdF "classique" basée sur la fiabilité et la maintenabilité, l'impact de facteurs extérieurs et, notamment, d'agressions sur la disponibilité opérationnelle est moins bien établi. Quelques approches traitent les facteurs extérieurs relativement au concept de survivabilité pour l'évaluation de la disponibilité notamment avec la considération de la vulnérabilité et de la susceptibilité. Par ailleurs, les actions visant à redonner des capacités fonctionnelles, appelées *recouvrement* sont vues comme une composante de la survivabilité au même titre que la maintenabilité pour la disponibilité.

Enfin, beaucoup d'approches ont été présentées et toutes se basent sur une phase de modélisation préalable à l'évaluation. Aussi, il convient de caractériser ces approches au regard de la méthodologie de construction des modèles supports des évaluations.

2.4 Méthodes de construction des modèles

L'évaluation de la disponibilité opérationnelle des systèmes repose sur l'utilisation de modèles permettant de reproduire le comportement des systèmes étudiés offrant ainsi la possibilité de caractériser les systèmes dès les premières phases de conception. Chaque technique offre la possibilité de modéliser des comportements plus ou moins complexes, moyennant la construction du modèle adéquat. Aussi, l'étape de construction des modèles est particulièrement importante puisqu'elle va conditionner l'adéquation des résultats (issus de l'analyse des modèles) avec la réalité du problème (cf. §2.2.1). En ce sens, des méthodologies de construction des modèles de disponibilité ont été développées afin de fournir un support à l'évaluation de la disponibilité. Basées sur les principales techniques que nous avons abordées à la section §2.2.2 (Chaînes de Markov, RdP Stochastiques et SANs), ces méthodes comportent toutes au moins deux étapes que sont la description *statique* et la description du comportement *dynamique* du système considéré.

2.4.1 Méthode basée sur une combinaison de modèles combinatoires et états-transitions

Les modèles combinatoires bien adaptés à la description des conditions de bon et mauvais fonctionnement trouvent leurs limites dans la description de comportement de type défaillance/réparation plus ou moins complexe que les modèles états-transitions sont plus à même de représenter. L'association de ces deux types de modèles permet donc une approche multi-niveaux avec des degrés d'abstraction plus ou moins forts. Typiquement, Trivedi *et. al* (K. Trivedi et al. 2006) proposent une démarche de modélisation pour l'évaluation de la disponibilité basée sur l'exploitation conjointe des blocs diagrammes de fiabilité (BDF) et des chaînes de Markov définissant ainsi une approche de modélisation par composition hiérarchique multi-niveaux. Les BDF permettent une approche de haut niveau pour la description du fonctionnement des systèmes. Les composants mis en oeuvre sont alors identifiés ainsi que leur dépendance (de type série/parallèle). Ensuite, les auteurs proposent la construction de la chaîne de Markov représentative du comportement des composants pour les évaluations autorisant la modélisation de comportement de type défaillance/réparation plus ou moins complexe. Les systèmes considérés sont supposés Markoviens et les évaluations sont analytiques. La disponibilité de chaque composant peut être calculée séparément. Enfin, sur la base du bloc diagramme de fiabilité, la disponibilité du système est obtenue. Cette approche multi-niveaux rend les modèles plus compréhensibles, évitant la construction d'une chaîne de Markov globale peu lisible. Elle nécessite cependant une hypothèse forte d'indépendance entre les composants au regard des défaillances, peu représentative des conditions réelles d'exploitation des systèmes.
Les réseaux de Petri qui offrent un pouvoir de modélisation plus étendu, notamment

en terme de dépendance entre les composants, sont eux aussi largement utilisés avec des modèles combinatoires. A ce titre, Malhotra et Trivedi, (M. Malhotra et K. Trivedi 1995) ont développé des algorithmes qui permettent de transformer les arbres de défaillances en RdPSG et SRN, sur la base des arbres de défaillances à événements répétés (FTRE - Fault Tree with Repeated Events) préalablement introduits dans (M. Malhotra et KS Trivedi 1994). Une autre contribution développée par Ereau (J-F Ereau 1997), associé RdPSG et arbres de défaillances. L'auteur propose une synchronisation originale des différents réseaux construits représentatifs du comportement de chacun des éléments constitutifs de l'arbre de défaillance. La modélisation est ainsi facilitée pour les ingénieurs en charge des études de sûreté. En effet, les arbres de défaillances constituent un outil largement utilisé dans le milieu industriel représentant les conditions menant à un événement redouté dans un formalisme largement compréhensible. La possibilité offerte par ces algorithmes de construire le modèle RdP équivalent constitue donc un outil d'analyse des propriétés de SdF autorisant une évaluation quantitative.

2.4.2 Méthode par affinement de modèles

Pour garantir les propriétés de SdF, les évaluation doivent être menées au plus tôt, dès la conception des systèmes. Il s'agit donc ici d'appréhender la SdF dès que les spécifications fonctionnelles sont connues comme le proposent Betous-Almeida et Kanoun, (C. Betous-Almeida et K. Kanoun 2004a) dans leur méthode de modélisation par affinements. L'approche proposée comporte trois étapes. La première, consiste en une construction d'un modèle basé uniquement sur les spécifications fonctionnelles de l'application, nommé modèle fonctionnel. Des règles permettent la transformation du modèle de haut niveau en un modèle plus détaillé. L'affinement peut être fait selon trois perspectives : décomposition des composants, affinement des états ou des événements et mise au point des distributions par la méthode des états fictifs dans le cas de systèmes non markoviens. Cette méthode permet de prendre en compte des comportements relativement complexes grâce au processus d'affinement du modèle de SdF et contourne le problème des systèmes non-markoviens par la méthode des états fictifs. Une bibliothèque de modèles permet de réduire l'effort de modélisation et les différents niveaux d'abstraction possibles dans la modélisation autorisent une évaluation dès la phase de conception.

2.4.3 Méthode intégrée à l'ingénierie des systèmes

Indispensable à tout programme, la SdF se doit d'être intégrée aux processus d'ingénierie des systèmes. Comme il a été souligné au premier chapitre (§1.4), il est nécessaire d'uniformiser les données utilisées en ingénierie système par la SdF et les autres disciplines pour réduire les efforts de modélisation. En ce sens, Beaudet *et. al*, (S.T. Beaudet, T. Courtney et W. Sanders 2006) proposent une approche d'ingénierie avec une méthode en deux étapes : une étape de description et une étape d'évaluation. La première étape de description correspond à l'écriture d'un document d'ingénierie système qui décrit le système, son comportement au regard des défaillances et de leur réparation, ainsi que les grandeurs à évaluer. La seconde étape revient à construire le modèle support aux

évaluations dans le formalisme des SANs. Cette seconde étape repose sur trois phases : la construction du modèle SAN, la définition de variables de récompenses (principe identique aux SRN, cf. § 2.2.2) et enfin, l'analyse du modèle. Cependant, si la première étape semble indispensable à la modélisation, les auteurs ne proposent aucun support à la description. De plus, comme dans la majorité des cas, les modèles de disponibilité présentés ne tiennent pas compte des facteurs extérieurs. Enfin, le passage d'une étape à une autre n'est pas détaillé et ne garantit donc pas l'adéquation de la description initiale avec le modèle support des évaluations.

2.4.4 Synthèse sur la construction des modèles

Peu de travaux présentent des méthodes de modélisation expliquant la nature des données nécessaires et les étapes permettant d'obtenir les modèles supports des évaluations. Les principales approches présentées ci-dessus couvrent tout ou partie du processus de modélisation. Plus ou moins tournées vers des applications industrielles, ces méthodologies présentent différents degrés de généricité et exploitent nécessairement les connaissances disponibles sur le système considéré. Éléments incontournables à la SdF (cf. §2.2.1), seuls Beaudet *et. al* considèrent la description du système dans leur méthodologie pour structurer les connaissances indispensables à la démarche de SdF.

2.5 Conclusion

Relativement au problème d'évaluation de la disponibilité opérationnelle en présence de défaillance, de dommage et de régénération, des réponses partielles sont apportées par les contributions de SdF classiques, d'une part, et dans les travaux axés sur la survivabilité, d'autre part. Dans les premiers, la prise en compte de facteurs extérieurs fait défaut. La disponibilité opérationnelle n'est fonction que de la fiabilité et de la maintenabilité vues comme des caractéristiques intrinsèques des systèmes souvent indépendantes des conditions d'exploitation. Des travaux particuliers comme ceux de Upadhya apportent partiellement une réponse en considérant des dommages mais leur impact physique n'est pas réellement pris en compte. Pour cela, les approches de survivabilité telles que celles proposées par Levitin semblent plus adaptées mais plus spécifiques au domaine d'application et la formulation particulière de la survivabilité ne fait pas le lien avec la disponibilité opérationnelle qui est une mesure reconnue de performance des systèmes, constituant un critère de choix dans les phases d'acquisition. Par ailleurs, les techniques de modélisation et d'évaluation de la communauté SdF et de la communauté survivabilité sont parfois communes (cf. les travaux de Liu, (Y. Liu, B.V. Mendiratta et S.Kishor Trivedi 2004, Yun Liu et Kishor Trivedi 2004) par exemple) mais restent le plus souvent dédiées n'autorisant donc pas la définition d'une méthodologie de modélisation générique. Toutefois, l'approche de modélisation proposée par Beaudet *et. al*, (S.T. Beaudet, T. Courtney et W. Sanders 2006), basée sur l'ingénierie système et l'utilisation des SANs, de par la flexibilité et la généricité qu'elle offre semble plus à même de répondre aux

exigences de l'ingénierie de régénération. La prise en compte simultanée de défaillances, de dommages et de régénération dans un contexte d'ingénierie des systèmes sur la base d'une méthodologie de modélisation générique et flexible nécessite cependant un effort d'unification des concepts à la base de ces considérations que sont fiabilité, vulnérabilité, maintenabilité, survivabilité et disponibilité.

Pour ce faire, nous proposons dans le chapitre suivant une méthodologie de modélisation pour l'évaluation de la disponibilité opérationnelle en présence de défaillances, de dommages et de régénération basée sur une approche unifiée défaillance/dommage. Cette approche repose sur une vision unifiée des concepts qui permettent d'appréhender défaillances et dommages (fiabilité/ survivabilité) ainsi que la régénération liée à la maintenabilité. Support à l'ingénierie de régénération, la méthodologie proposée repose tout d'abord sur un modèle de données dérivé des modèles de données d'ingénierie système permettant ainsi de structurer la connaissance nécessaire à la construction des modèles d'évaluation. Dans une deuxième étape, cette approche tire profit des techniques de modélisation états-transitions et, plus particulièrement, du pouvoir de modélisation des SANs offrant la possibilité de représenter des comportement complexes intégrant dépendances et interactions indispensables à la prise en considération du mécanisme de dommage. Constituant un bon support aux simulations de Monte Carlo, les SANs, nous donnent également la possibilité de représenter des processus stochastiques généraux tels que ceux utilisés par Upadhya, (K. Upadhya et N. Srinivasan 2005) pour modéliser les agressions.

Chapitre 3

Méthodologie de modélisation pour l'Ingénierie de Régénération

Dans ce chapitre, nous présentons le principe d'unification à la base de la méthodologie. Cette unification des différents concepts nous conduit à proposer dans une première partie un atome de modélisation générique du comportement des composants en présence de défaillances, de dommages et de régénération ainsi qu'un atome de modélisation générique représentatif quant à lui du comportement des fonctions. La méthodologie globale de modélisation est présentée et les principes à la base de la construction du modèle structurel sont détaillés.

3.1 Introduction

La mise en oeuvre d'une ingénierie de régénération répondant aux besoins industriels identifiés au chapitre I requiert le développement d'un ensemble de processus basés sur différentes méthodes correctement outillées afin de construire une méthodologie de modélisation cohérente avec l'ingénierie des systèmes et répondant aux besoins d'évaluation de la disponibilité opérationnelle.
Aussi, afin de répondre à cette problématique, nous introduisons dans ce troisième chapitre une méthodologie de modélisation des systèmes basée sur une approche unifiée défaillance/dommage. Développée sur la base des modèles de SdF abordés au chapitre II, cette méthodologie intègre également des résultats de travaux axés sur la survivabilité.
L'approche proposée est fondée sur une vision cohérente des défaillances, des dommages et de la régénération pour une modélisation conjointe nous conduisant à définir un atome de modélisation générique du comportement des composants. Pour proposer une approche générique globale, nous définissons également un atome de modélisation générique du comportement des fonctions. Ensuite, nous définissons le modèle structurel, qui fournit un cadre pour la formalisation des connaissances nécessaires à la construction des modèles atomiques représentatif d'un système. Ce modèle structurel permet de formaliser l'ensemble de la connaissance nécessaire à l'évaluation, allant de la description du système à la définition du scénario opérationnel.

3.2 Unification défaillance/dommage pour la régénération : un atome de modélisation du comportement des composants et des fonctions

En nous basant sur le parallèle entre défaillance et dommage établi par Perrin *et. al* (J. Perrin, P. Esteve et X. Le Vern 2001a) ainsi que sur l'analyse des travaux existants présentée au deuxième chapitre, l'unification défaillance/dommage proposée se matérialise tout d'abord par l'unification des concepts inhérents à la régénération conduisant à identifier les liens existants entre fiabilité, maintenabilité, vulnérabilité, susceptibilité, survivabilité et disponibilité. Ce positionnement nous amène ensuite à considérer défaillance et dommage dans la modélisation. Le comportement en présence de défaillance et de dommage est alors introduit, unifiant ainsi les concepts. De la même manière, la régénération et sa modélisation seront abordées sur la base des concepts de maintenance et de réparation des dommages au combat (RDC[1]).

[1]Réparation essentielle, pouvant être improvisée et/ou temporaire, effectuée rapidement dans des conditions de combat, afin de remettre en service le matériel endommagé ou immobilisé, (NATO 1994)

3.2.1 Principe de l'unification

Le chapitre II nous a permis d'appréhender les concepts socles de la SdF ainsi que la survivabilité dans un objectif d'évaluation de la disponibilité opérationnelle. Aussi, en nous basant sur les conclusions du chapitre II, nous proposons de retenir des différents concepts les considérations suivantes pour développer notre approche unifiée :

- la disponibilité est évaluée sur la base de la fiabilité et de la maintenabilité des systèmes,
- fiabilité et maintenabilité sont des caractéristiques intrinsèques qui dépendent des dispositions constitutives,
- la survivabilité dépend de la vulnérabilité, de la susceptibilité et de la fiabilité des systèmes,
- la survivabilité qui caractérise l'aptitude d'un système à terminer sa mission peut être caractérisée comme une mesure particulière de la disponibilité opérationnelle : "Aptitude d'une entité à être en état d'accomplir une fonction [...] pendant un intervalle de temps donné" (cf. définition 2.3) si l'intervalle de temps considéré correspond à la mission assignée au système,
- la régénération est concernée aussi bien par les défaillances que par les dommages et englobe ainsi les différents concepts tels que la recouvrabilité et la maintenabilité utilisés respectivement dans les études de disponibilité et de survivabilité,
- la régénérabilité joue nécessairement un rôle dans la survivabilité, dans le sens où l'aptitude d'un système à terminer sa mission va également être fonction de son aptitude à récupérer des capacités fonctionnelles après l'occurrence d'une défaillance ou d'un dommage.

L'unification proposée relativement aux différents concepts manipulés nous permet donc d'établir les relations entre les concepts telles que présentées à la figure 3.1, (M. Monnin et al. 2006). La prise en compte de la régénération dans les études de disponibilité néces-

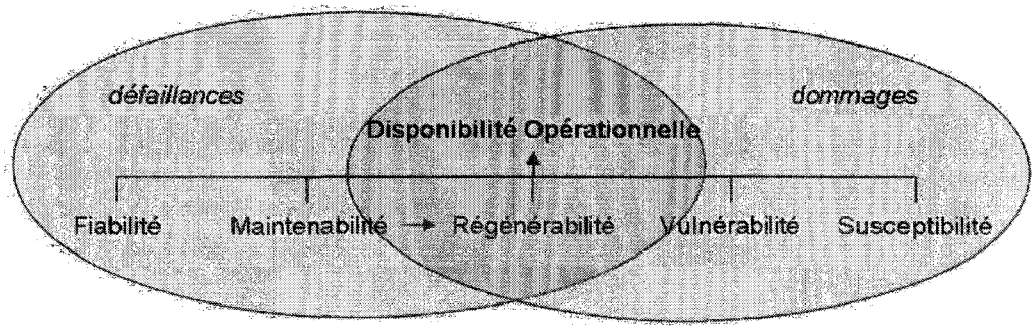

FIG. 3.1 – Sûreté de fonctionnement et Survivabilité - relation entre les concepts.

site donc d'avoir une approche globale permettant de considérer différents points de vue relativement aux systèmes considérés. Trois axes sont donc retenus pour représenter le comportement des composants en présence de défaillances, de dommages, et de régéné-

ration : la fiabilité, la vulnérabilité, et la régénérabilité. Dans un premier temps, fiabilité et vulnérabilité sont abordées relativement au parallèle entre défaillance et dommage permettant ainsi une unification défaillance - dommage dans la modélisation. Ensuite, la régénération, qui se situe à l'intersection de la maintenance et de la RDC est considérée sur un principe d'unification maintenance - RDC. Le rôle du soutien logistique dans la régénération sera présenté, nous permettant ainsi de proposer une modélisation cohérente de la régénération avec la représentation des défaillances et des dommages sur la base d'un atome générique de modélisation des composants. Cet atome de modélisation est construit sur les hypothèses suivantes, basées sur les approches présentées à la section 2.2.2 :

- l'atome de modélisation est un modèle de type états-transitions,
- le nombre d'états considérés est fini et l'atome est donc représentable par un graphe d'état où les sommets représentent les états et les arcs représentent les transitions,
- défaillances, dommages et régénération sont des processus stochastiques à la base de la description du comportement des systèmes au regard de l'évaluation de la disponibilité opérationnelle.

3.2.2 Unification défaillance - dommage

Modélisation de la fiabilité et maintenabilité

Pour développer l'unification défaillance/dommage, l'atome de modélisation proposé s'appuie tout d'abord sur les représentations connues du comportement des composants au regard des défaillance et de la maintenance. En effet, notre approche n'a de sens que si elle intègre ces représentation afin de ne pas être réductrice. Aussi, à l'instar des représentations rencontrées dans la littérature, la fiabilité sera caractérisée par le taux de défaillance qui représente la fréquence à laquelle un composant passe d'un état de bon fonctionnement à un état de panne. La défaillance a donc un impact fonctionnel dans le sens où elle conduit le composant dans un état où la fonction n'est plus assurée. Dans une représentation état-transition le comportement en présence de défaillance est capturé en représentant le composant par deux états souvent notés : "ok" et "panne", la transition de l'un à l'autre étant fonction du taux défaillance. Pour caractériser la disponibilité, on introduit la maintenabilité qui représente la transition entre l'état "panne" et l'état "ok". L'occurrence de l'état "panne" résulte donc de l'occurrence d'une défaillance et le retour à l'état "ok" résulte donc de la réalisation d'une action de maintenance représentée par la maintenabilité du composant. Le comportement correspondant peut être représenté par un graphe d'état G tel que :
$G = (V, E)$ où $V = \{v_1, v_2, ..., v_n\}$ (|V| = n) sont les sommets représentant les états, et $E = \{e_1, e_2, ..., e_m\}$ (|E| = m) les arcs représentant les transitions entre les états. Un arc e de l'ensemble E est défini par une paire ordonnée de sommets. Lorsque e = (u, v), on dira que l'arc e va de u à v. On dit aussi que u est l'extrémité initiale et v l'extrémité finale de e. On a alors, $V = \{v_1, v_2\}$ et $E = \{e_1, e_2\}$ avec $v_1 = ok$, $v_2 = panne$, $e_1 = (v_1, v_2) = défaillance$ et $e_2 = (v_2, v_1) = maintenance$ le graphe correspondant est représenté figure 3.2.

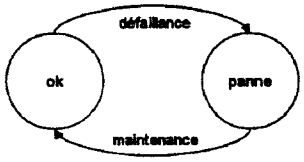

FIG. 3.2 – Graphe d'état d'un composant pour l'évaluation de la disponibilité

Cette représentation du comportement en présence de défaillances et de maintenance que nous adoptons constitue l'élément de base à partir duquel l'application du principe d'unification nous conduit à définir l'atome de modélisation des composants.

Modélisation de la vulnérabilité : représentation des dommages

Au comportement précédemment définit nous proposons donc d'intégrer une représentation de la vulnérabilité des composants. La vulnérabilité s'attache à caractériser le comportement d'un système, sous-système composant au regard des agressions qu'il peut subir. Aussi, comme l'état "panne" résulte de l'occurrence d'une défaillance, les dommages résultent de l'occurrence d'une agression, (DoD 1980). Cependant, si l'état "panne" représente l'impact fonctionnel d'une défaillance, les états représentatifs des dommages doivent nous permettre de rendre compte de :

1. l'impact physique des agressions,
2. l'impact fonctionnel des agressions.

Pour ce faire, nous nous appuyons sur les travaux de Perrin, (J. Perrin, P. Esteve et X. Le Vern 2001b) dans lesquels les agressions impliquent soit la destruction du composant (dommage majeur), soit sa détérioration (dommage mineur). La destruction résulte d'agressions qui ont un impact physique sur le composant, le rendant inapte à remplir sa fonction. Dans le contexte de la régénération, la destruction revient à la perte totale du composant dans le sens où un composant détruit ne pourra subir aucune action de régénération. En effet, par analogie à la maintenabilité, un composant détruit a une régénérabilité nulle : le composant n'a plus "d'aptitude à être remis en service pour terminer sa mission".

La prise en compte de la détérioration quant à elle apporte une flexibilité dans la caractérisation des dommages. Les études de vulnérabilité qui déterminent l'effet des agressions sur les composants permettent de déterminer l'impact physique et fonctionnel d'une agression. Un composant "détérioré" peut donc être caractérisé par un niveau de performance fonctionnelle et par un niveau de performance technique représentatif de la régénérabilité du composant.

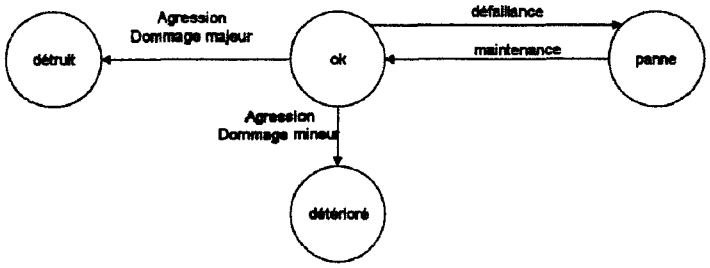

FIG. 3.3 – Graphe d'état d'un composant unifiant défaillance et dommage

Pour rendre compte des agressions et des dommages qui en résultent, nous proposons d'ajouter au modèle de disponibilité en présence de défaillances, deux états représentatifs de la destruction et de la détérioration.
Nous définissons donc le comportement des composants en présence de dommage de la manière suivante :

- l'endommagement d'un composant résulte de l'occurrence d'une agression,
- l'endommagement est caractérisé par deux états possibles après l'occurrence de l'agression : "détruit" ou "détérioré",
- les deux états sont caractérisés par un niveau d'atteinte physique et par un niveau d'atteinte fonctionnelle (lié à la fonction supportée par le composant), pour chaque composant, ces niveaux doivent être évalués pour chaque agression possible,
- pour chaque agression, chaque composant est caractérisé par :
  - une probabilité d'être atteint par l'agression (représentative de la susceptibilité du composant à l'agression et liée à sa localisation dans le système),
  - une probabilité d'être détérioré,
  - une probabilité d'être détruit.
- par expertise il est possible de considérer une propagation des dommages au sein d'un système qui va notamment dépendre de la localisation des composants dans le système (G. Levitin et A. Lisinanski 2000). La propagation des dommages entre composants permet de représenter la notion de dommage étendu (J. Perrin, P. Esteve et X. Le Vern 2001a) selon laquelle une agression peut conduire à l'endommagement de plusieurs composants qui n'ont pas nécessairement de lien fonctionnel, en raison du *chemin de l'agression*. Les conséquences fonctionnelles de telles agressions peuvent donc être multiples.

Cette première étape dans l'unification défaillance - dommage pour la modélisation des systèmes se matérialise donc par l'ajout des états "détruit" et "détérioré" au modèle classique de disponibilité précédemment représenté à la figure 3.2. Le nouveau modèle proposé est donné à la figure 3.3, avec V={ok, panne, détérioré, détruit} et E={défaillance, maintenance, agression (dommage mineur), agression (dommage majeur)}

Le comportement décrit à la figure 3.3, permet donc de rendre compte de la fiabilité, de la maintenabilité ainsi que de la vulnérabilité des composants. Nous allons main-

tenant aborder la régénération afin d'introduire la régénérabilité dans la définition du comportement des composants.

3.2.3 Unification maintenance - Réparation des Dommages au Combat

Dans les approches de disponibilité, la maintenabilité des composants est le plus souvent caractérisée par le taux de réparation μ. Les actions de maintenance correspondantes pour l'évaluation de la disponibilité permettent un retour dans l'état "ok" du composant. Cette hypothèse devient très forte dans le contexte de la régénération et ce pour trois raisons :

1. la régénération étend le concept de RDC aux défaillances et aux dommages. La régénération a un caractère temporaire[2] et vise uniquement à redonner au système les capacités opérationnelles suffisantes pour qu'il poursuive sa mission. Cela sous-entend que la maintenance classique visant à restaurer les systèmes intervient entre les missions.
2. les moyens logistiques pour la régénération ne sont pas ceux de la maintenance et conditionnent la régénération.
3. les dommages que peuvent subir les systèmes affectent leur régénérabilité (cf. section 3.2.2) de sorte que la nature de l'action de régénération possible va, d'une part, dépendre du niveau d'atteinte physique du composant représenté par son état courant et, d'autre part, faire passer le composant dans un état différent de l'état nominal.

Aussi, pour différencier maintenance et régénération, nous nous appuyons tout d'abord sur le rôle du soutien logistique (cf. section 1.2.2 au chapitre I). Relativement aux définitions données des NTIs, la régénération relève du NTI 1. Les opérations sont effectuées avec des moyens limités, par les utilisateurs des matériels eux-mêmes ou par des structures légères de proximité (ELI : Equipe Légère d'Intervention). Relativement à cette définition nous proposons de considérer trois niveaux d'actions pour la régénération :

- une régénération automatique (qui ne nécessite pas d'intervention humaine)
- une régénération par l'équipage
- une régénération par les ELI au contact.

Une action de régénération est donc caractérisée par le personnel, les moyens ainsi que le temps nécessaire à sa réalisation. Sur la base des travaux sur la régénération présentés dans (J. Perrin, P. Esteve et X. Le Vern 2001b), nous proposons trois actions de régénération :

- l'échange,
- le dépannage,
- la reconfiguration.

[2] le caractère temporaire de la régénération se définit au même titre que le caractère temporaire d'une action de maintenance palliative tel que défini dans (AFNOR 2001). Cela n'exclut cependant pas des actions de régénération à caractère définitif (en référence à la maintenance corrective (AFNOR 2001)) quand cela est possible.

Chacune de ces actions de régénération ne conduit pas nécessairement au même état : le nouvel état atteint après régénération doit rendre compte de l'impact fonctionnel de la régénération (retour à un état fonctionnel), mais va également dépendre de l'état physique du composant. La régénération nécessite donc d'introduire de nouveaux états au modèle de la figure 3.3 pour assurer une vision cohérente défaillance, dommage et régénération. La disponibilité n'est donc plus uniquement fonction de la fiabilité et de la maintenabilité mais doit prendre en compte notamment les trois types d'actions de régénération proposés qui permettent au système de retrouver des capacités opérationnelles. Pour ce faire, nous allons détailler la modélisation de chacune des actions de régénération afin de définir comment elles peuvent être introduites dans la modélisation du comportement des composants.

Modélisation de la régénération

La première action de régénération introduite dans la modélisation correspond à l'échange. Réaliser une action d'échange nécessite de pouvoir accéder au composant pour réaliser les opérations de pose et de dépose (au sens de la maintenabilité). Cette action est donc uniquement possible si le composant est en panne. En effet, l'état "panne" est défini par une perte de performances fonctionnelles uniquement, les performances techniques n'étant pas affectées par la défaillance. Enfin, de par sa nature l'échange, qui consiste à remplacer le composant en panne, est représenté par la transition "panne" $\rightarrow$ "ok".

La seconde action de régénération que nous définissons est appelée dépannage. Le dépannage correspond à une action simple (réparation) qui vise à redonner un fonctionnement dégradé temporaire au composant. Cette action nécessite de pouvoir accéder au composant (au sens de la maintenabilité) mais ne nécessite pas la dépose du composant ; elle peut donc être envisagée à partir de l'état "panne" (pour lequel les performances techniques sont nominales) et à partir de l'état "détérioré" (pour lequel les performances techniques n'empêchent pas l'accessibilité au composant). Pour rester cohérent avec la dualité performances fonctionnelles (PF) - performances techniques (PT) qui permet de rendre compte de l'impact physique des agressions, on considère que le dépannage d'un composant en panne le mènera dans un état "régénéré1" tel que :
$PF(panne) < PF(régénéré1) < PF(ok)$ et
$PT(panne) = PT(régénéré1) = PT(ok)$
De la même façon, le dépannage d'un composant "détérioré" le fait passer dans l'état "régénéré2" tel que :
$PF(détérioré) < PF(régénéré2) < PF(ok)$ et
$PT(détérioré) = PT(régénéré2) < PT(ok)$, avec
$PT(régénéré1) \neq PT(régénéré2)$

Enfin, nous définissons la reconfiguration qui constitue la troisième action possible de régénération. Par définition, (A. Toguyéni, P. Berruet et E. Craye 2003), la reconfiguration qui est considérée comme un processus en réponse à une défaillance en phase d'exploitation du système, consiste en une réorganisation de la structure matérielle et de

la partie commande du système pour permettre au système de continuer à fonctionner après l'occurrence d'une défaillance. Par extension, cette définition est appliquée en cas de défaillance ou de dommage. Pour représenter la reconfiguration, nous nous basons sur les considérations suivantes :

- la reconfiguration met en oeuvre deux composants (C1 et C2) qui participent à deux fonction différentes (F1 et F2),
- la perte du composant C1 suite à une défaillance ou une agression, va affecter (perte ou dégradation) la fonction F1 à laquelle il participe.

La reconfiguration va permettre au composant C2 de se substituer au composant C1 atteint et de participer à la fonction F1 pour qu'elle retrouve un état de disponibilité pour le système. Ainsi, deux types de reconfiguration sont considérés :

1. **Type 1** : le composant C2 reconfigure C1 et participe alors à F1 et F2. F2 voit éventuellement son état modifié du fait que C2 n'est plus dédié uniquement à cette fonction. (e.g. un calculateur se voit affecter une charge de calcul supplémentaire pour une autre fonction par reconfiguration. Les deux calculs (F1 et F2) sont assurés mais vont prendre plus de temps).
2. **Type 2** : le composant C2 reconfigure C1 et participe à F1 mais n'est plus en mesure d'assurer F2.

La reconfiguration s'exprime donc à deux niveaux. Tout d'abord, au niveau des composants, elle implique un changement d'état du composant C2. Pour rendre compte de l'effet de la reconfiguration sur la fonction F2, (changement d'état de C2), nous introduisons un état supplémentaire au niveau des composants : l'état "en reconfiguration". Par ailleurs, la reconfiguration de type 1 en raison de la *double* utilisation du composant C2 peut conduire à une modification de la fiabilité du composant en accélérant le processus de dégradation du composant d'une part et peut également modifier sa vulnérabilité si son utilisation pour une autre fonction l'amène à une exposition accrue aux agressions. La reconfiguration s'exprime également au niveau des fonctions du système puisqu'elle va permettre par l'intermédiaire du composant C2 de redonner à la fonction F1 des capacités opérationnelles. Enfin, les états relatifs à la reconfiguration ("régénéré1", "régénéré2" et "en reconfiguration") correspondent à des états de disponibilité du composant caractérisés par un niveau de performance fonctionnelle particulier qui peut également subir des défaillances et des dommages.

Nous pouvons maintenant représenter le comportement global d'un composant en présence de défaillances, de dommages et de régénération. Les états introduits relativement à la régénération, viennent donc compléter le graphe d'état de la figure 3.4, de telle sorte que V={ok, panne, détérioré, détruit, régénéré1, régénéré2, en reconfiguration} et E={défaillance, défaillance1, défaillance2, défaillance3, échange, agression (dommage mineur), agression (dommage majeur), agression (dommage mineur) 1, agression (dommage majeur) 1, agression (dommage mineur) 2, agression (dommage majeur) 2, agression (dommage mineur) 3, agression (dommage majeur) 3, reconfiguration, réparation 1, réparation 2} où,
défaillance $\Longleftrightarrow$ok $\rightarrow$ panne
défaillance1 $\Longleftrightarrow$régénéré1 $\rightarrow$ panne

défaillance2 $\Longleftrightarrow$ régénéré2 $\rightarrow$ panne
défaillance3 $\Longleftrightarrow$en reconfiguration $\rightarrow$ panne
échange$\Longleftrightarrow$ panne $\rightarrow$ ok
agression (dommage mineur) $\Longleftrightarrow$ ok $\rightarrow$détérioré
agression (dommage majeur) $\Longleftrightarrow$ ok $\rightarrow$détruit
agression (dommage mineur) 1$\Longleftrightarrow$ régénéré1$\rightarrow$ détérioré
agression (dommage majeur) 1$\Longleftrightarrow$ régénéré1 $\rightarrow$ détruit
agression (dommage mineur) 2$\Longleftrightarrow$ régénéré2 $\rightarrow$ détérioré
agression (dommage majeur) 2$\Longleftrightarrow$ régénéré2 $\rightarrow$ détruit
agression (dommage mineur) 3$\Longleftrightarrow$ en reconfiguration$\rightarrow$ détérioré
agression (dommage majeur) 3$\Longleftrightarrow$ en reconfiguration$\rightarrow$ détruit
reconfiguration $\Longleftrightarrow$ ok $\rightarrow$ en reconfiguration
réparation 1 $\Longleftrightarrow$ panne $\rightarrow$ régénéré1
réparation 2 $\Longleftrightarrow$ détérioré $\rightarrow$ régénéré2

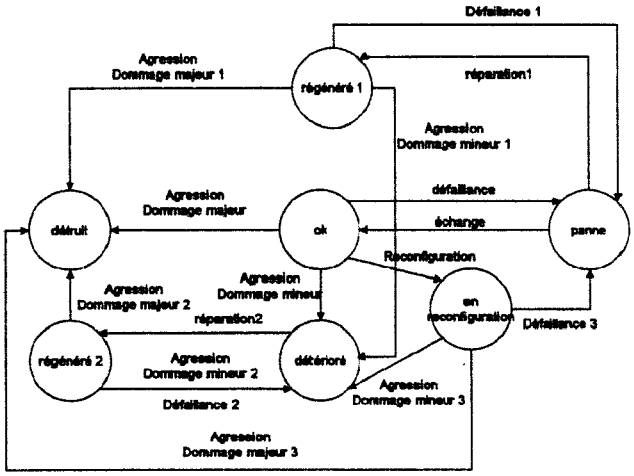

FIG. 3.4 – Représentation générique sous forme d'un graphe d'état du comportement en présence de défaillance, de dommage et de régénération

Afin de compléter cette approche générique de modélisation des systèmes, nous définissons également un atome de modélisation des fonctions supportées par les composants. Pour définir cet atome, nous nous basons sur la définition de la survivabilité proposée au chapitre I, (définition 1.1). Selon cette définition, les capacités opérationnelles du système (supportées par les fonctions du système) peuvent être :

- entières,
- partielles,
- servir uniquement à protéger l'équipage.

Chacun de ces niveaux peut être traduit par un état particulier représentatif du niveau de performance de la fonction. Aussi, pour être complet nous considérons la perte

totale de la fonction. Les états de la fonction correspondants seront donc respectivement : Nominal (ou OK) , Dégradé, Secours et Panne. Le graphe d'état correspondant avec V={OK, Dégradé, Secours , Panne} est donné à la figure 3.5.

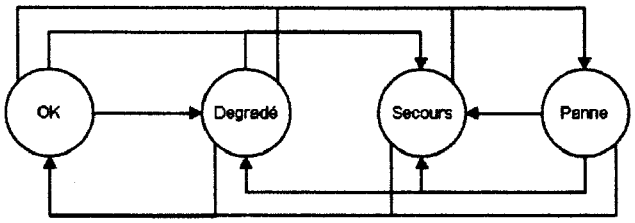

FIG. 3.5 – Représentation générique sous forme d'un graphe d'état du comportement des fonctions

Les transitions entre les états d'une fonction ne sont volontairement pas étiquetées. Les transitions entre les états de la fonction sont définies à partir de l'état des différents composants qui la supportent.

La contribution méthodologique de ces travaux s'appuie sur cette proposition de représentation du comportement des composants et des fonctions en présence de défaillance, de dommages et de régénération. L'ensemble de la méthodologie support de l'ingénierie de régénération peut maintenant être développée.

La méthodologie de modélisation

La méthodologie support de l'Ingénierie de Régénération est constituée de trois grandes phases. La première reprend et étend un point clé de la démarche de SdF qui s'attache à définir la connaissance du système nécessaire pour mener à bien les études de SdF. L'objectif de cette première étape dans la modélisation est double :

1. tout d'abord elle permet de guider la modélisation du système en définissant les éléments à considérer pour l'évaluation,
2. ensuite, étant basée, d'une part, sur un principe de description systémique utilisé en ingénierie système et sur le modèle de données de l'ingénierie système, d'autre part, elle assure la cohérence de la description du système au sein d'un programme en manipulant les mêmes données que les autres processus impliqués.

Cette première étape nous permet de définir un atome de modélisation générique du comportement des composants intégrant défaillances, dommages et régénération.
Sur la base de cet atome de modélisation, la seconde étape correspond à la construction du modèle dynamique supporté par les Stochastic Activity Networks. Une composition hiérarchique des modèles permet de spécifier le comportement des fonctions supportées par les composants. Des variables de récompense sont ensuite définies relativement aux grandeurs de SdF à évaluer.
Par ailleurs, des règles de construction dérivées du modèle structurel permettent de

garantir la cohérence de la description du système avec le modèle dynamique en contraignant la construction de ce dernier.
Enfin, le modèle est utilisé au travers de simulations qui permettent d'évaluer statistiquement les variables de récompenses.

L'ensemble de la démarche est schématisé à la figure 3.6.

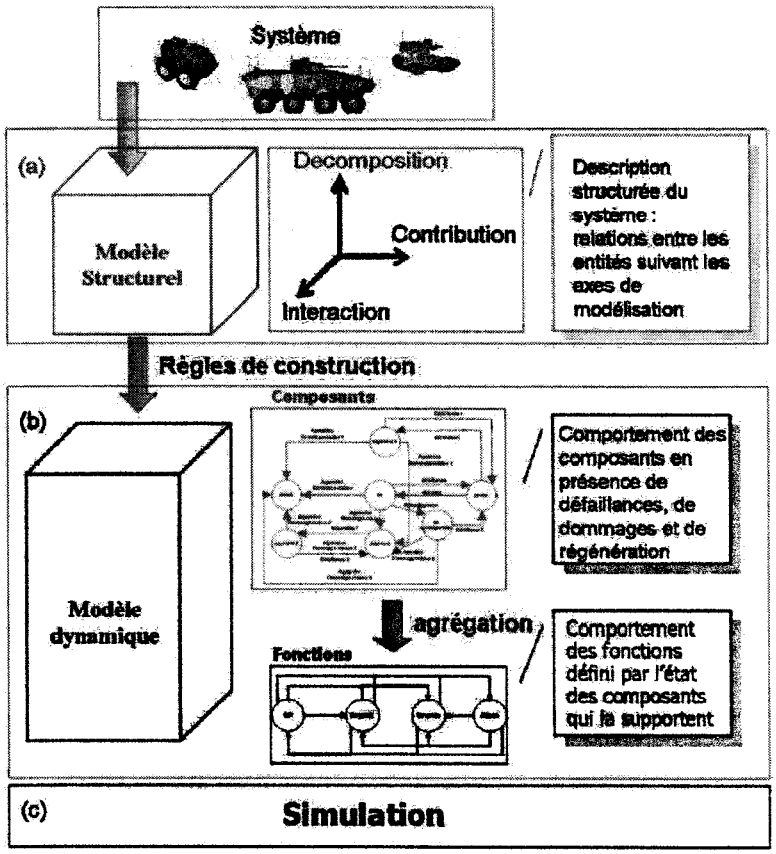

FIG. 3.6 – Synoptique de la démarche de modélisation

3.2.4 Conclusion

L'approche unifiée défaillance dommage proposée dans ce mémoire se justifie par le manque de méthodes et d'outils permettant d'aborder conjointement la fiabilité et la vulnérabilité des systèmes indispensables à la considération de la régénération, au sein d'une même évaluation de performance de SdF. Nous avons présenté dans cette première partie comment les différents concepts inhérents aux défaillances, d'une part, et aux dommages, d'autre part, pouvaient être rapprochés de manière à proposer une modélisation commune du comportement des composants. Ainsi, sur la base de travaux

relatifs aux études de dommages, nous avons proposé une représentation des agressions et des dommages intégrée à la représentation des défaillances plus classique. De la même manière, la considération de la maintenance et de la maintenabilité dans les modèles de disponibilité avec la réparation des dommages subis au combat nous a permis de définir une typologie de la régénération. La régénération compte donc trois types d'actions en réponse aux défaillances et/ou dommages et qui dépendent du soutien logistique associé au système principal. Dans la prochaine section, le premier modèle proposé dans la méthodologie : le modèle structurel, est présenté. Cette section développe les principes à la base de la représentation statique des systèmes qui intègre les données nécessaires à la construction du modèle dynamique pour l'évaluation de la disponibilité opérationnelle.

3.3 Le modèle structurel

La démarche de SdF passe nécessairement par une phase de description du système concerné afin de regrouper la connaissance disponible et indispensable à la compréhension des mécanismes de défaillances et, a fortiori, de dommages. Cette étape primordiale fait toutefois souvent défaut dans les travaux rencontrés dans la littérature. Dans un objectif de généricité et d'intégration de l'Ingénierie de Régénération à l'Ingénierie système, nous définissons tout d'abord un cadre méthodologique, support de la description des systèmes. Donnant les étapes à suivre et les éléments à considérer pour appréhender le comportement des systèmes, cette première étape conduit à la construction d'un modèle de données statique : *le modèle structurel* correspondant à une description structurée du système. Cette description structurée est basée sur la notion d'entités et de relations. Le système est décrit par différentes entités en un ensemble de relations. Ces relations sont soit entre les entités de même nature, soit entre entités de types différents. Le formalisme UML, (OMG 2003) et plus particulièrement les diagrammes de classes ont été choisis pour représenter le modèle structurel. En effet, les diagrammes de classes représentent des données statiques sous la forme d'entité-relation, permettant ainsi de définir les entités décrivant le système et d'identifier les relations entre ces entités. De plus, le groupe NEXTER system avec lequel nous avons travaillé, se tourne de plus en plus pour ses outils informatiques supports aux différents ateliers d'ingénierie système, vers des outils basés sur le langage UML voire SysML[3], pour la partie descriptive du système considéré (e.g. l'outil Rhapsody®. de la société Teleogic - http ://modeling.telelogic.com/). Par ailleurs, bien que disponible aujourd'hui, les spécifications du langage SysML, n'étaient pas encore disponibles à la construction des différents modèles présentés dans la suite. Ces différents éléments ont donc motivé le choix du langage UML comme support au modèle structurel. Ainsi, la construction d'un modèle statique a donc pour objectif principal de structurer toute la connaissance nécessaire à la construction et au paramétrage des différents atomes représentatifs du comportement des systèmes.

[3]http ://www.sysml.org/

3.3.1 Principe de représentation des systèmes en IS

Le modèle structurel est basé sur une approche d'ingénierie système. En ce sens, le système considéré ou système à étudier est d'abord abordé suivant trois points de vue utilisés en IS :

- le point de vue fonctionnel,
- le point de vue organique (physique/technique),
- le point de vue opérationnel.

En effet, en IS, la définition d'un système nécessite premièrement d'identifier ce que le système doit faire (fonctionnel) pour répondre à sa finalité (mission) et, ensuite, on identifie les organes pour le faire, (J-P. Meinadier 2002). Suivant la logique de modélisation adoptée, nous donnons le diagramme de classe de la figure 3.7 comme première représentation de ces différents points de vue. Les entités décrivant le système sont donc : la mission, les fonctions, les organes. Les classes correspondantes ne comprennent pas d'attributs, cette représentation conceptuelle permet d'illustrer les points de vue à travers lesquels les systèmes seront décrits. Les classes représentant les entités seront précisées à mesure que nous détaillerons la modélisation.

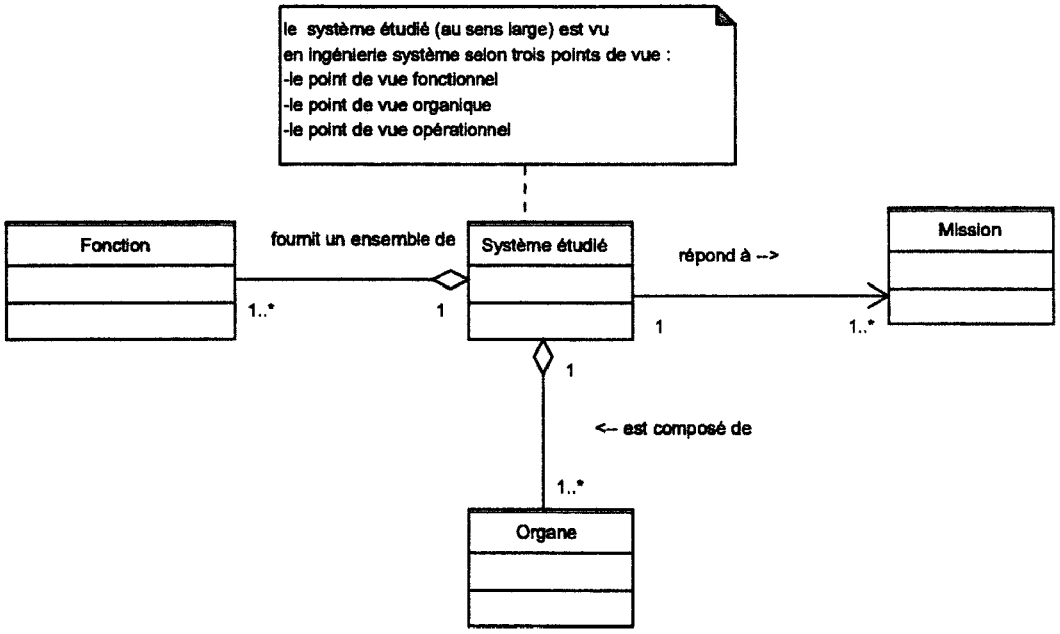

FIG. 3.7 – Les points de vue de description des systèmes

Pour les différentes relations considérées, nous nous basons sur les travaux de Tomala, (F. Tomala 2002) qui propose une représentation des systèmes dans le contexte des modèles de produits suivant trois axes de modélisation qui sont :

- un axe de décomposition,

- un axe d'interaction,
- un axe de contribution,

Chaque axe nous permet de définir un ensemble de relation Ri relatif aux entités du système (organe, fonction, mission). La description d'un système débute donc par le définition de l'ensemble des éléments qui le composent au travers des relations de décomposition. Chaque entité peut être décomposée pour affiner la connaissance du système. Ce principe générique laisse une grande liberté dans le niveau de granularité choisi pour l'étude dans la mesure où il y a toujours cohérence entre les niveaux de décomposition choisis pour les différentes entités. Nous considérerons donc trois types de décomposition :

- une décomposition fonctionnelle - relation $R1$,
- une décomposition organique - relation $R2$,
- une décomposition opérationnelle - relation $R3$.

Relativement au diagramme de classe de la figure 3.7, le principe de décomposition peut être représenté pour chaque entité par une relation d'agrégation[4]. La figure 3.8, rappelle les décompositions pour chacune des entités par une relation d'agrégation dans le formalisme UML.

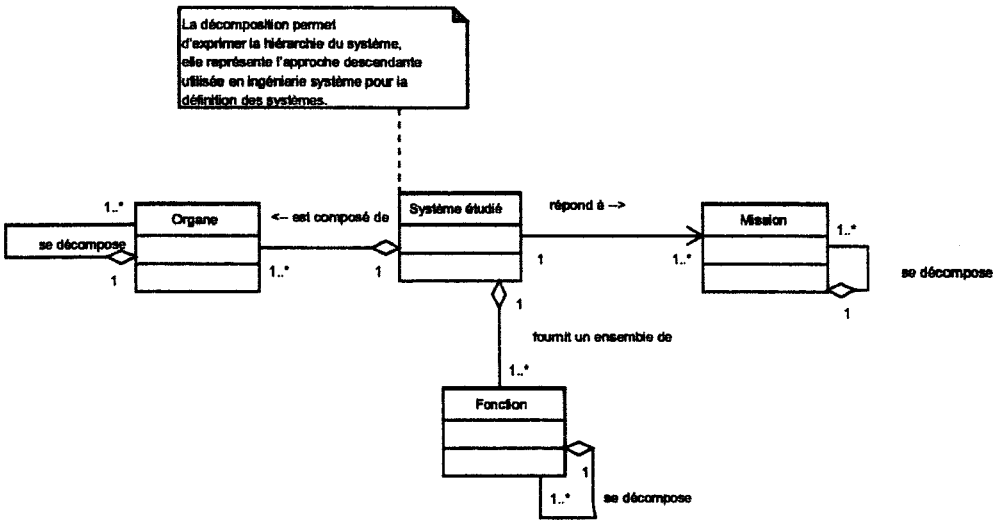

FIG. 3.8 – Décomposition des systèmes.

L'axe des interactions intervient sur le même type d'entité et ne concerne pas toutes les entités. En effet, cet axe permet de définir des relations telles que les dépendances fonctionnelles, les interactions topologiques entre les organes ou encore la notion d'inter-

[4]En UML, l'agrégation est une relation « composé-composant » ou « partie de » dans laquelle les objets représentant les composants d'une chose sont associés à un objet représentant l'assemblage (ou l'agrégation) entier, elle permet donc de représenter la notion de décomosition

changeabilité relative à la maintenabilité. Les relations d'interactions considérées seront donc :

- une interaction fonctionnelle - relation $R4$,
- une interaction d'interchangeabilité - relation $R5$,
- une interaction topologique - relation $R6$,

A ce stade de la description, les interactions sont identifiées sur la base du diagramme de la figure 3.7 par des classes d'associations tel que présenté à la figure 3.9. Nous utilisons ici des classes d'associations afin de pouvoir dans la suite caractériser les relations d'interaction en définissant des attributs à chacune des classes d'association pour préciser l'interaction.

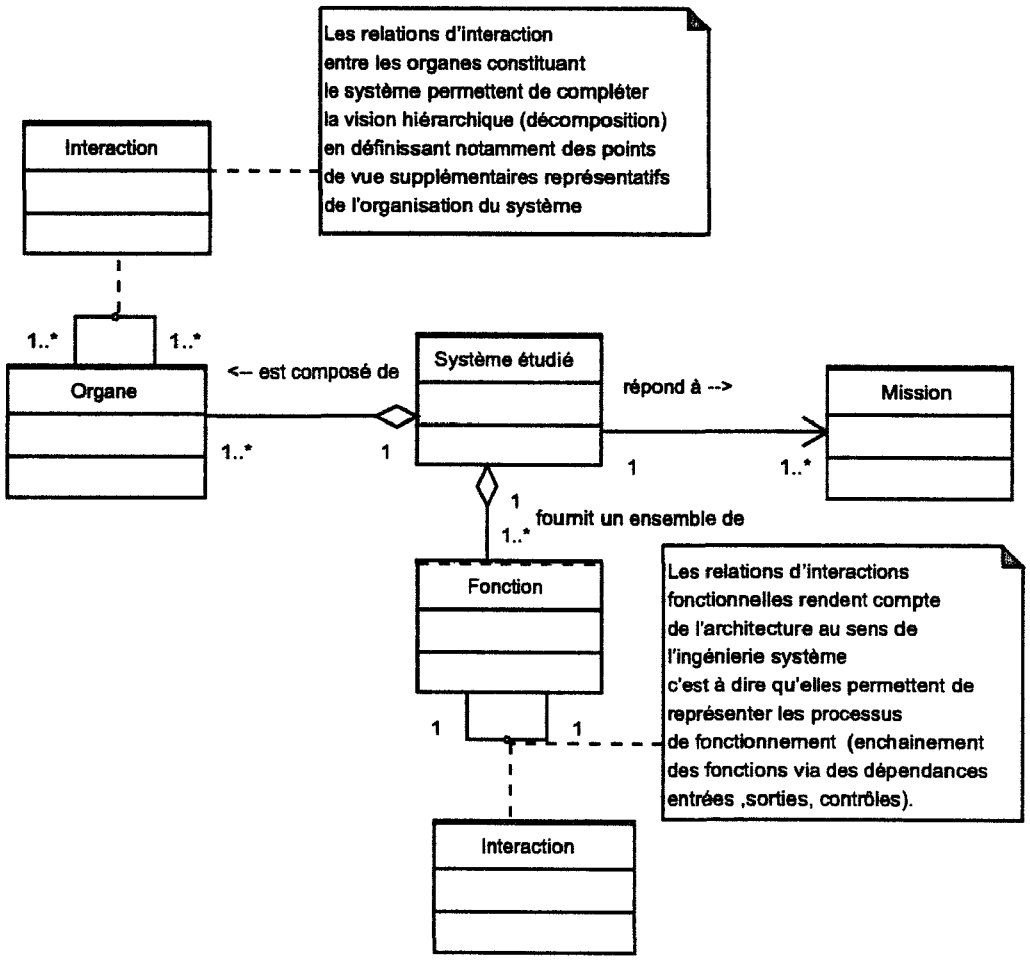

FIG. 3.9 – Relations d'interaction entre les fonctions et entre les organes

Enfin, pour formaliser les relations entre les différentes entités, à l'instar des travaux de Tomala, nous considérons des relations de contribution entre les entités. Les relations de contribution permettent de relier les différents points de vue adoptés en ingénierie système sur les systèmes (organique, fonctionnel, opérationnel) en définissant les relations entre les points de vue. En ce sens, l'axe de contribution représente tout d'abord la notion suivante : *un système est composé d'organes supports à des fonctions et répond à un besoin opérationnel exprimé en terme de mission.* Cela nous permet donc de définir dans un premier temps les relations de contribution suivantes :

- les fonctions contribuent à (remplissent) la mission assignée au système - relation $R7$,
- les organes contribuent (supportent) aux fonctions du système - relation $R8$,
- la mission (par le biais des agressions potentielles) contribue au (agit sur le) fonctionnement des organes - relation $R9$.

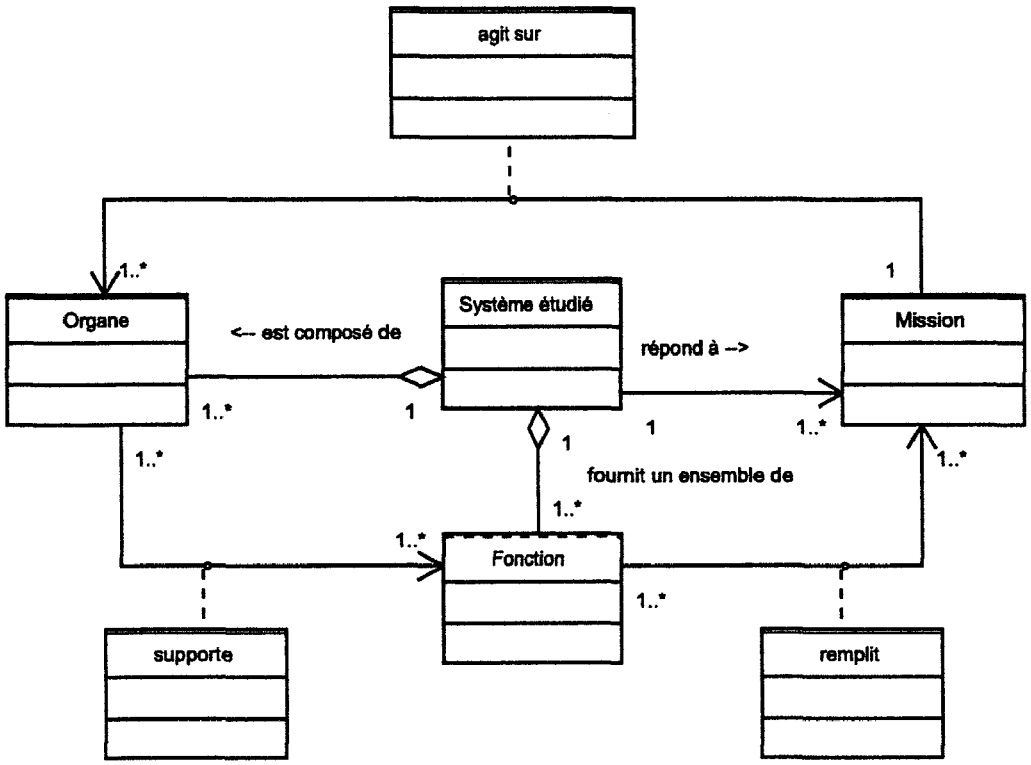

FIG. 3.10 – Relations de contribution entre les entités.

Ces relations reportées à la figure 3.10, sont représentées par des classes d'association ("remplit", "supporte" et "agit sur") de manière à pouvoir dans la suite les préciser par la définition des attributs de chacune des classes.

Nous avons donné le cadre général de description des systèmes formalisé par un ensemble de diagrammes de classe représentant les entités (très générales) à considérer. Nous allons maintenant aborder plus en détail les différentes relations afin de montrer comment ces dernières permettent de représenter tous les aspects indispensables à la construction d'un modèle dynamique pour l'évaluation de la disponibilité opérationnelle des systèmes d'armes.

3.3.2 Modèle structurel et modèle de données de l'AFIS

La section précédente nous a permis de donner les différents points de vue utilisés pour la représentation de la connaissance nécessaire pour les évaluations de disponibilité. Les diagrammes de classes correspondant restent à un niveau très abstrait donnant une représentation conceptuelle. Pour être exploitables dans la suite de la méthodologie, il est nécessaire de préciser chacune des relations *Ri* par d'autres diagrammes plus précis. Pour ce faire, les entités sont tout d'abord précisées au regard du modèle de données proposé par l'AFIS, (GT Modélisation et Outils 2002) dont nous redonnons le diagramme de classe correspondant à la figure 3.11. Selon le modèle de l'AFIS, les fonctions corres-

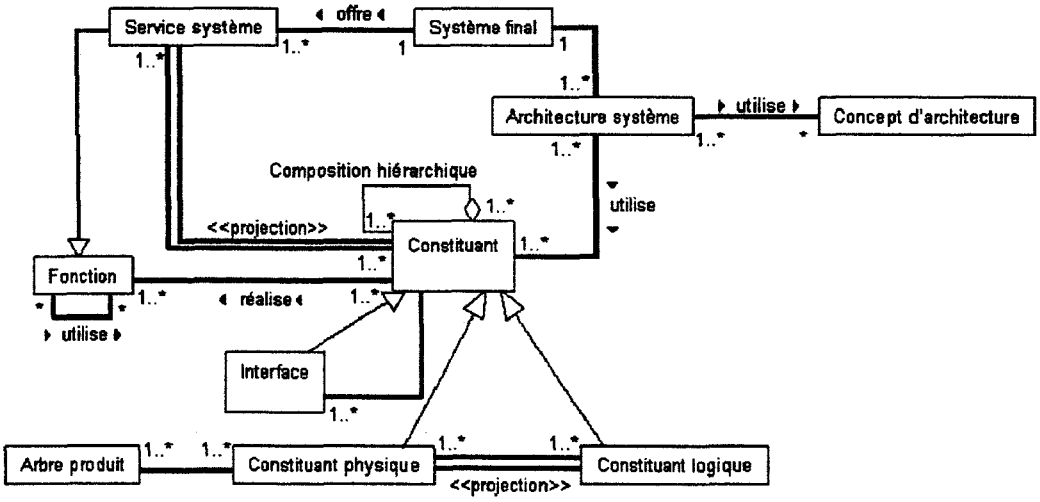

FIG. 3.11 – Modèle de données, Vue Architecture

pondent à une *transformation d'entrées en sorties.* Ces fonctions se déclinent en *service système.* Un service système correspond à un service fourni par le système à la frontière entre le système et son environnement et produisant un résultat défini répondant à un besoin. Par ailleurs, les fonctions organisées en services système sont supportées par des *constituants.* Ces constituants sont définis comme des *éléments d'architecture issus d'un choix de décomposition système.* Un constituant peut être logique ou physique; dans notre cas, les entités considérées sont des constituants physiques : *constituants concrets réalisables, offrant des fonctions et possédant des caractéristiques et propriétés.* Le mo-

dèle structurel proposé nous permet donc de préciser certaines relations définies dans le modèle de données de l'AFIS et d'en considérer d'autres afin d'orienter la connaissance pour l'ingénierie de régénération. Par exemple, la décomposition organique du modèle structurel va permettre de rendre compte à la fois de la *"composition hiérarchique"* entre constituants et de la relation de structuration entre l'architecture et les constituants. De la même manière, la relation de contribution des organes aux fonctions précise la relation *"réalise"* entre les constituants et les fonctions. Suivant la même logique, les relations d'interaction fonctionnelle vont préciser la relation *"utilise"* définie entre les fonctions dans le modèle de l'AFIS. Par ailleurs, le modèle structurel étend le modèle proposé par l'AFIS en offrant la possibilité de décrire la mission et ses interactions avec le système en introduisant la classe "Mission" et les différentes relations qui en découlent.

Afin d'avoir un exemple support à la description des différentes relations, nous nous appuierons sur un exemple d'architecture organico-fonctionnelle. Les principaux aspects des architectures militaires seront précisées. En effet, les diagrammes de classe précédemment présentés fixent le cadre général de la construction du modèle structurel, qui permet à l'approche proposée d'être générique. Pour les besoins de l'ingénierie de régénération dans un contexte militaire, les diagrammes de classes correspondants aux différentes relations de décomposition, d'interaction et de contribution seront orientés relativement à notre problématique plus particulière.

Une architecture de Système de Systèmes (SdS) est composée d'un ensemble d'éléments de manoeuvre (EM), chaque EM est doté d'un ensemble de plates formes et chaque plate forme est composée d'un ensemble de constituants. Un EM est caractérisé par sa fonction ou capacité opérationnelle qui lui est assignée. En effet, l'architecture *organique* d'un système de système est définie pour répondre à une capacité opérationnelle globale attendue. Ainsi, chaque élément de manoeuvre se verra assignée une fonction du type[5] :

- commandement,
- combat indirect,
- combat direct,
- renseignement.

Pour réaliser ces fonctions, l'EM est doté d'un ensemble de plates-formes caractérisées par leur type. Les plates-formes correspondent aux différents véhicules qui peuvent être classés selon qu'ils sont : Léger (e.g. VAB[6]), Moyen (e.g. VBCI[7]) ou Lourd (e.g. Char Leclerc). Chaque plate-forme peut supporter jusqu'à trois types de fonctions opérationnelles : les fonctions socles, les fonctions principales et les fonctions secondaires. Les fonctions socles sont communes à toutes plates-formes, chaque plate-forme a une fonction principale et peut éventuellement supporter une ou plusieurs fonctions secondaires. Pour de telles architectures, une mission est définie en termes de phases, elles-mêmes com-

[5]Les fonctions définies ici pour les EM correspondent aux fonctions allouées aux EM dans le cadre de la définition des SGTIA (Sous-Groupements Tactiques Interarmes) dans la BOA

[6]Véhicule de l'Avant Blindé

[7]Véhicule Blindé de Combat d'Infanterie

posées de séquences. La mission se caractérise également par le type de conflit concerné, le type d'opposition rencontrée ainsi que la durée globale de la mission. Les séquences portent également une information temporelle (proportion de la mission) et environnementale (liée aux agressions).

L'exemple retenu pour illustrer le modèle structurel correspond à un SGTIA[8] constitué d'un EM de renseignement lui même doté de trois plates-formes chacune décomposées en 2 sous-systèmes (notés SS_1 à 6). Deux des trois plates-formes ont une fonction principale d'OBSERVATION, et la troisième à une fonction principale de FEU. Cette architecture est présentée à la figure 3.12. Relativement à cet exemple, nous allons préciser

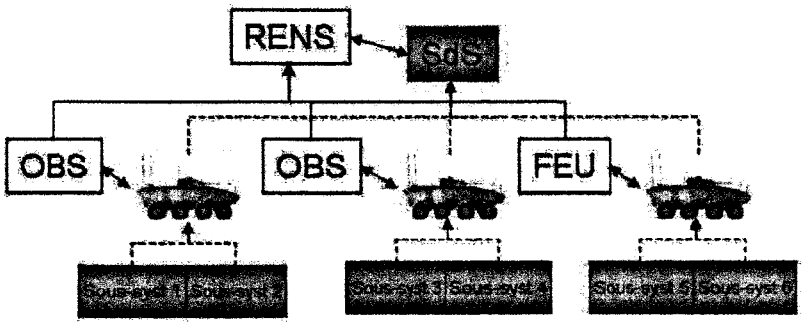

FIG. 3.12 – Exemple d'architecture de système de systèmes.

les différentes relations à la base du modèle structurel en commençant par les relations de décomposition.

3.3.3 Les relations de décomposition

Nous présentons dans cette section les différentes relations de décomposition $R1$ à $R3$. Les relations génériques modélisées suivant l'axe de décomposition sont donc respectivement pour chacun des types d'entités les relations :

$$Rn(a,b) : a \textit{ est composé de } b \text{ avec,}$$

$a \in A$ (A : ensemble des entités de même nature : constituant, fonction, mission),
$b \in A$ et n nature de l'entité (variant de 1 à 3).
Le niveau de décomposition choisi (i.e. nombre de niveaux) dépendra d'éléments tels que, la connaissance disponible, le niveau de précision souhaité, la politique de régénération (composant candidat à l'échange, à la réparation, ...).
De plus, à mesure que les entités seront précisées dans les décompositions, nous introduirons les différents éléments de description plus spécifiques à l'Ingénierie de Régénération au travers de l'exemple.

[8]Sous Groupement Tactique Interarmes

La décomposition fonctionnelle - Relation $R1$

A l'échelle du système de systèmes, l'architecture fonctionnelle de la figure 3.12 peut être décomposée en deux niveaux : les capacités opérationnelles et les fonctions opérationnelles. On a dans l'exemple considéré une capacité opérationnelle de *Renseignement* composée de trois fonctions opérationnelles : deux fonctions d'*Observation (1 et 2)* et une fonction *Feu*[9], ce qui donne les relations $R1$ suivantes :

- $R1(Renseignement, Observation\_1)$,
- $R1(Renseignement, Observation\_2)$,
- $R1(Renseignement, Feu)$,

avec $A = \{Renseignement, Observation\_1, Observation\_2, Feu\}$.
Le formalisme UML choisi pour représenter les relations nous permet de représenter différents niveaux d'abstraction dans la décomposition par le biais des *généralisations*. En effet, le diagramme de classe choisi pour représenter les fonctions opérationnelles correspond à une généralisation de fonctions qui peuvent prendre différents types : fonctions socles, principales ou secondaires. De plus, pour compléter les définitions de l'entité fonction à travers la décomposition fonctionnelle, à chaque fonction opérationnelle est associée son état. L'ensemble des états possibles est le même pour toutes les fonctions opérationnelles et les états correspondent à un niveau de performance de la fonction (cf. figure 3.5). Le diagramme de classe correspondant à l'ensemble de la décomposition fonctionnelle est reporté à la figure 3.13.

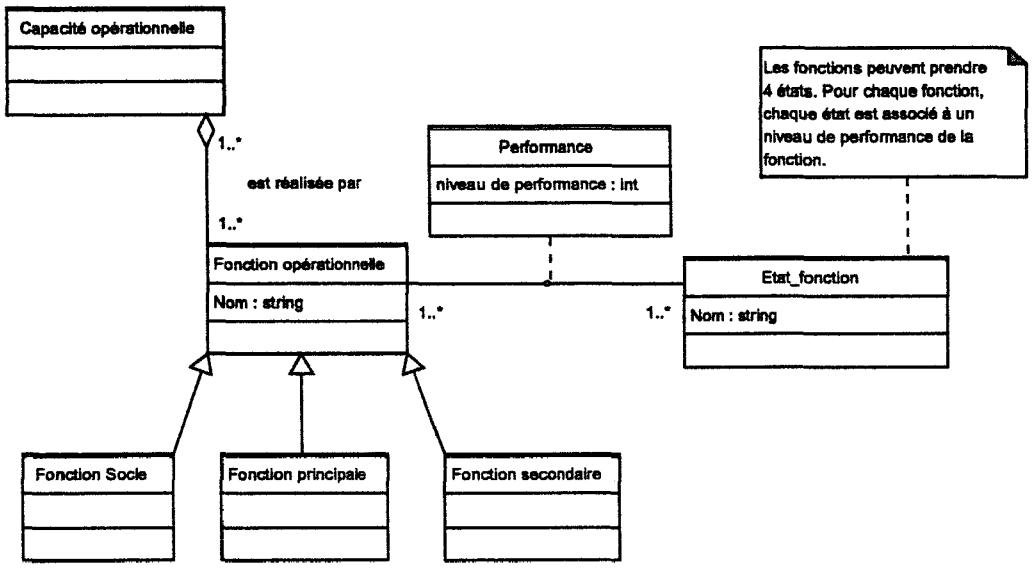

FIG. 3.13 – Diagramme de classe relatif aux relations de décomposition fonctionnelle

[9]La désignation "fonction Feu" correspond aux capacités de tir.

La décomposition organique - Relation *R2*

Relativement à notre problématique, la décomposition organique compte quatre niveaux pour représenter les systèmes de systèmes militaires. Chaque constituant est également caractérisé par son taux de défaillance, dans la mesure où l'on considère que la fiabilité est une caractéristique intrinsèque du constituant. Comme les fonctions, les constituants peuvent prendre un ensemble d'états caractérisés par un niveau de performances fonctionnelles et par un niveau de performances techniques relatifs aux fonctions techniques qui déterminent sa régénérabilité. On notera *e* l'ensemble des états possibles pour les constituants avec :

e={ok, panne, détérioré, détruit, régénéré1, régénéré2, en reconfiguration}

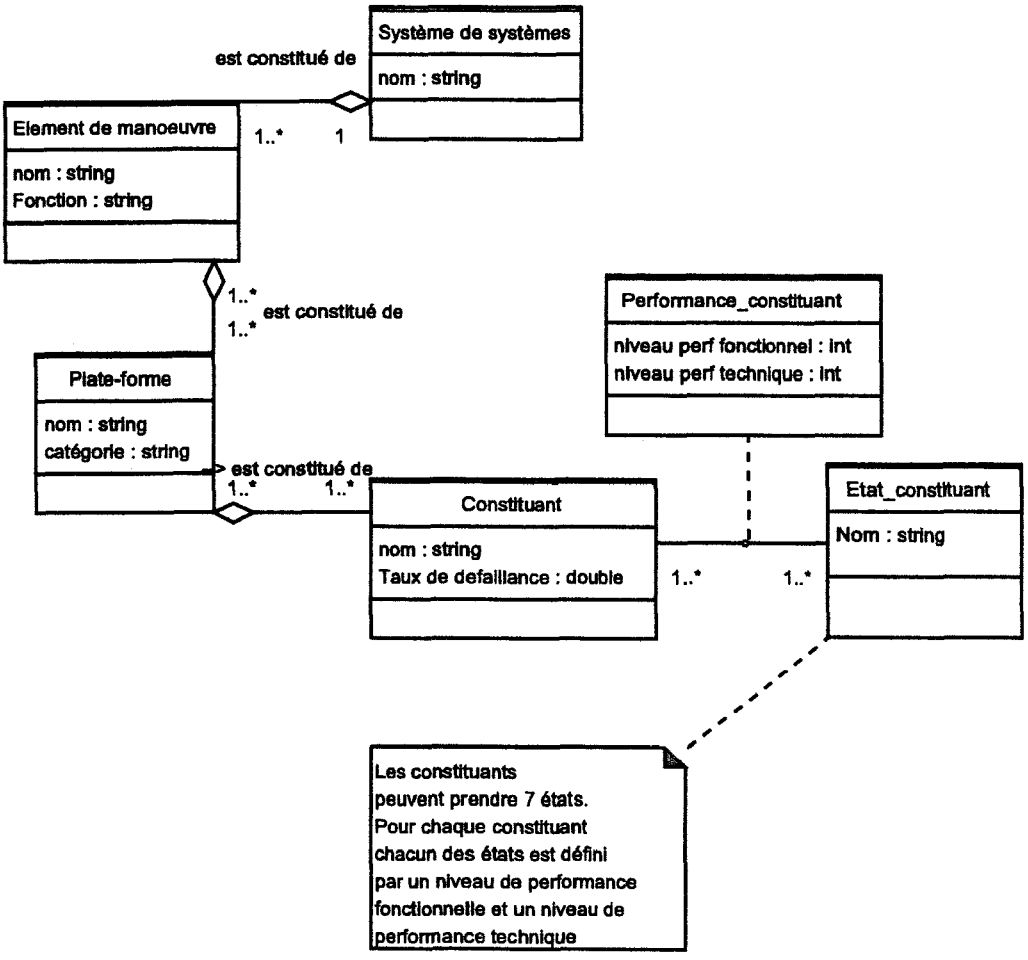

FIG. 3.14 – Diagramme de classe relatif aux relations de décomposition organique

Pour continuer l'exemple abordé à la section 3.3.3, si on considère un SGTIA constitué d'un EM de renseignement lui même doté de trois plates formes chacune décomposées en 2 sous-systèmes (notés SS_1 à 6), on obtient les relations de décomposition $R2$ suivantes :

- $R2(SGTIA,\ EM\_Renseignement)$,
- $R2(EM\_Renseignement,\ Plate\ forme\ OBS1)$,
- $R2(EM\_Renseignement,\ Plate\ forme\ OBS2)$.
- $R2(EM\_Renseignement,\ Plate\ forme\ FEU)$.
- $R2(Plate\ forme\ OBS1,\ SS\_1)$.
- $R2(Plate\ forme\ OBS1,\ SS\_2)$.
- $R2(Plate\ forme\ OBS2,\ SS\_3)$.
- $R2(Plate\ forme\ OBS2,\ SS\_4)$.
- $R2(Plate\ forme\ FEU,\ SS\_5)$.
- $R2(Plate\ forme\ FEU,\ SS\_6)$.

La décomposition opérationnelle - Relation $R3$

Le dernier point de vue abordé suivant l'axe de décomposition concerne le point de vue opérationnel. La décomposition opérationnelle rend compte de la structure de la mission et plus largement du contexte opérationnel avec la considération des agressions. Le diagramme de classe correspondant est reporté à la figure 3.15.

Comme pour les points de vue organique et fonctionnel, la décomposition proposée pour le point de vue opérationnel, concerne les applications militaires mais ne remet pas en cause le principe de décomposition valide dans tous les contextes. Le contexte opérationnel considéré ici à travers la prise en compte des agressions que peuvent subir les systèmes, se matérialise donc dans le diagramme de classe par une classe "agression". Cette classe permet de définir la catégorie des agressions considérée ainsi que sa probabilité d'occurrence. Une catégorie d'agression a une seule probabilité d'occurrence par séquence.

3.3.4 Les relations d'interactions

L'axe d'interaction permet de considérer des relations d'interactions entre les entités de même nature et de même niveau de décomposition. Suivant cet axe, la relation $R4$ représente les interactions fonctionnelles et les relations $R5$ et $R6$ concernent les constituants. On notera comme suit les relations d'interactions :

$$Rp(a,b) : a\ est\ en\ interaction\ avec\ b \text{ avec,}$$

$a \in A$ (A : ensemble des entités de même nature : constituant, fonction, mission),
$b \in A$ et
p nature de l'entité (variant de 4 à 6).

L'interaction fonctionnelle - Relation $R4$

La relation d'interaction fonctionnelle permet d'exprimer les dépendances entre les fonctions opérationnelles. Une dépendance est particulière et unique entre 2 fonctions

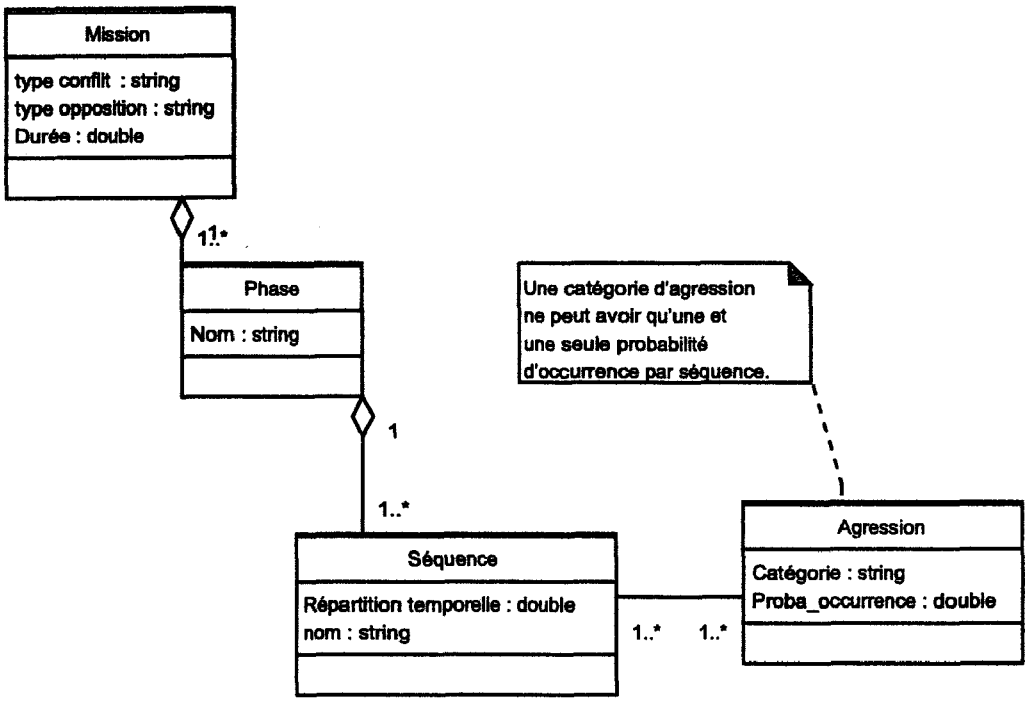

FIG. 3.15 – Diagramme de classe relatif aux relations de décomposition opérationnelle

et rend compte notamment de la notion de causalité entre deux fonctions. Elle permet donc de représenter des liens existant entre les fonctions, identifiés en terme de flux dans l'analyse fonctionnelle. Le diagramme de classe correspondant aux relations d'interactions entre les fonctions est donné à la figure 3.16. La relation d'interaction entre fonctions $R4$ est définie telle que :

$$R4(a, b) : a \textit{ est en interaction avec } b \text{ avec,}$$

a *et* $b \in A^2$ (A : ensemble des fonctions)
Considérons par exemple les fonctions "Viser/Pointer" et "Armer" qui participent à la fonction "Tirer" (cf. figure 3.17), le lien de type "entrée/sortie" entre ces deux fonctions constitue la relation d'interaction $R4(Viser/Pointer, Armer)$.

Les interactions entre constituants - relation $R5$ et $R6$

Nous avons identifié deux types d'interactions possibles entre les constituants : une interaction de type "interchangeabilité" ($R5$) qui peut intervenir sur la régénérabilité des systèmes et une interaction "topologique" ($R6$) liée à l'architecture du système qui permet de rendre compte de la localisation des constituants dans un système. Le diagramme

de classe de la figure 3.18, représente les interactions entre les constituants de manière générale et la figure 3.19 précise ces relations.

En ingénierie système, comme le système principal et le système de soutien sont conçus simultanément, les capacités d'interchangeabilité au sein d'un système ont donc un impact direct sur son système de soutien et également sur sa régénérabilité. L'interchangeabilité entre deux constituants est donc considérée comme un type d'interaction. Elle est caractérisée par le personnel nécessaire, l'outillage et le délai requis. Elle intervient également au niveau du stock relatif à une régénération par échange des constituants considérés. On définit donc la relation $R5$ telle que :

$$R5(a,b) : a \textit{ est interchangeable avec } b \text{ avec,}$$

a *et* $b \in A^2$ (A : ensemble des constituants).

La représentation d'interactions topologiques se base sur la définition d'ensembles topologiques caractérisés notamment par leur dimension et le nombre de constituants. Au sein de chaque ensemble topologique sont également définis des voisinages (figure 3.19). Ces voisinages permettent de caractériser les interactions liées à la topologie. Un voisinage caractérise l'interaction entre 2 constituants A et B. Cette représentation permet d'introduire différents types de dépendances liés à la présence d'une interaction :

- un dommage sur A peut conduire à un endommagement de B (proximité des constituants), l'état de B va donc dépendre de l'état de A, ou
- un dommage sur A peut conduire soit à la défaillance de B, soit à une modification du taux de défaillance de B.
- Un dommage sur B peut conduire à un endommagement de A (proximité des constituants), l'état de A va donc dépendre de l'état de B, ou
- un dommage sur B peut conduire soit à la défaillance de A, soit à une modification du taux de défaillance de A.

Chacune de ces interactions peut éventuellement être probabiliste.

Nous pouvons maintenant développer le dernier axe de modélisation qui complète ainsi la description des systèmes en définissant les relations de contribution entre les entités de nature différente (cf. figure 3.10).

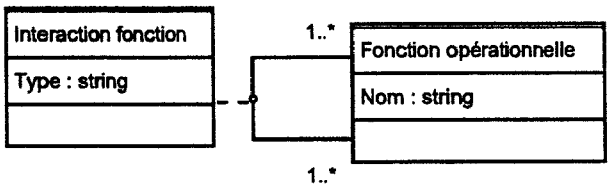

FIG. 3.16 – Diagramme de classe des relations d'interaction fonctionnelle

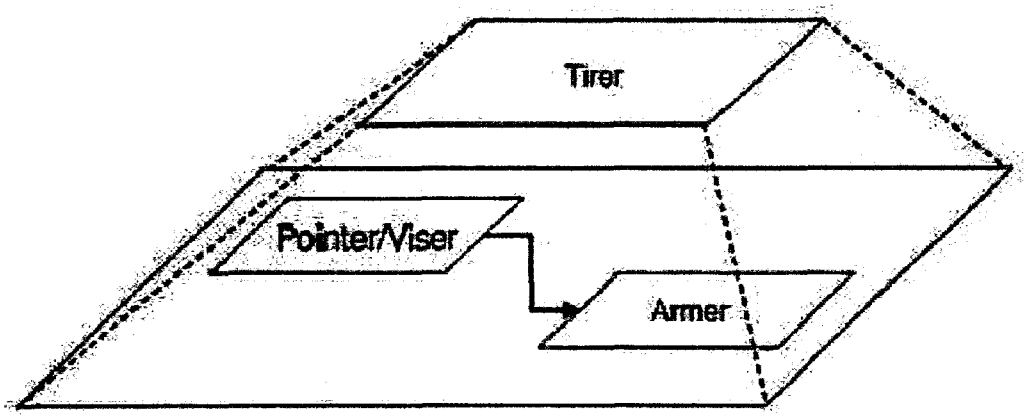

FIG. 3.17 – Exemple de liens entre fonctions dans l'analyse fonctionnelle

3.3.5 Les relations de contribution

Relativement au principe d'ingénierie système présenté à la section 3.3.1, nous présenterons tout d'abord la contribution des fonctions à la mission (*"identifier ce que le système doit faire (fonctionnel) pour répondre à sa finalité (mission)"*), ensuite nous détaillerons la contribution des constituants aux fonctions (*"les organes pour le faire"*) et, enfin, nous exposerons comment l'axe des contributions permet de considérer l'impact du contexte opérationnel à travers la relation de contribution de la mission sur les constituants.

La contribution des fonctions à la mission - relation $R7$

L'utilisation des différentes plates-formes au sein d'un scénario opérationnel est définie par le diagramme de contribution des fonctions à la mission (figure 3.20). On définit avec la classe association "participe" la relation de contribution telle que :

$$R7(a, b) : a \textit{ contribue à } b \text{ avec,}$$

$a \in A$ (A : ensemble des fonctions),
$b \in B$ (B : ensemble des séquences). Cette relation est caractérisée par les éléments suivants dans la mesure où ils sont connus et quantifiables :

- On peut introduire une *flexibilité* de la fonction pour la séquence traduisant l'importance de la fonction pour la séquence. Trois niveaux de flexibilité sont définis dans (J. Perrin, P. Esteve et X. Le Vern 2001b) : primordiale, importante, souhaitable. Cette flexibilité peut, si elle est introduite, avoir un effet sur la disponibilité opérationnelle dans le sens où la perte de fonctions avec des flexibilités différentes n'aura pas le même impact sur la disponibilité opérationnelle (e.g. la perte d'une fonction primordiale conduira à un arrêt de la mission alors que la perte d'une fonction souhaitable n'induira qu'une perte de performance).

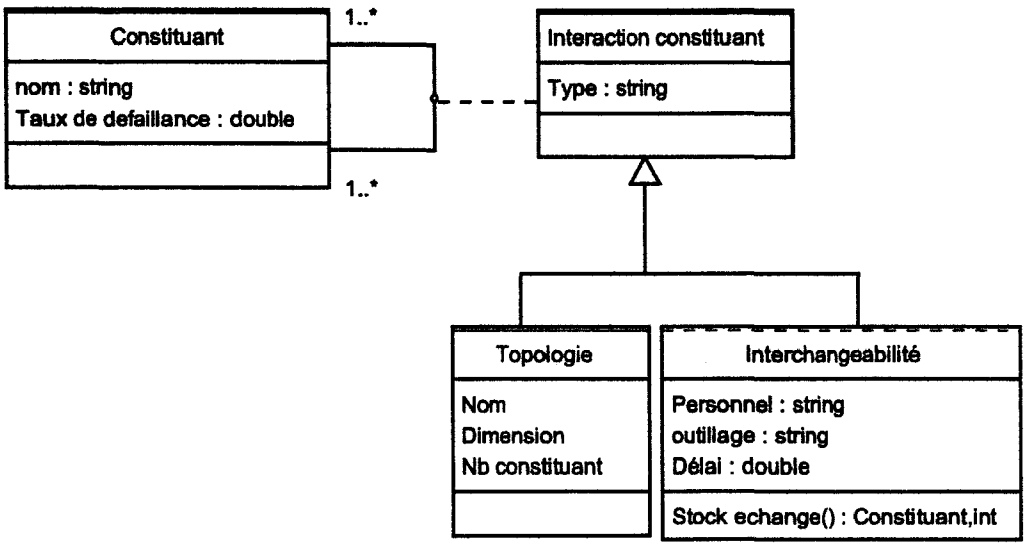

FIG. 3.18 – Diagramme de classe des relations d'interaction entre constituants (niveau conceptuel)

- Comme pour la flexibilité, il peut être intéressant de préciser la réalisation d'une séquence en définissant l'état minimum nécessaire pour commencer la séquence (attribut "état début") ainsi que l'état minimum pour mener à bien la séquence (attribut "état fin") relativement aux états possibles d'une fonction (E={nominal, dégradé, secours, panne}).

La contribution des constituants aux fonctions - relation $R8$

Le diagramme de la figure 3.21 représente les relations suivant l'axe de contribution entre les constituants et les fonctions. Un ensemble de capacités opérationnelles étant alloué au système de systèmes, chacune de ces capacités opérationnelles est supportée par un élément de manoeuvre. Les capacités opérationnelles sont réalisées par les fonctions opérationnelles qui sont supportées par les plates formes de la manière suivante :

- chaque plate forme supporte un ensemble de fonctions socles,
- chaque plate forme supporte une fonction principale,
- chaque plate forme peut également supporter une ou plusieurs fonctions secondaires.

Si les fonctions socles, principales et secondaires sont affectées aux plates formes, au sein des plates-formes, ces fonctions sont effectivement supportées par l'ensemble des constituants de la plate forme. Ainsi, pour chacun des types de fonctions opérationnelles (socle, principale et secondaire), l'état de la fonction est déterminé en fonction de l'état de chacun de ses constituants supports (relation " dépend de "). Cette relation consti-

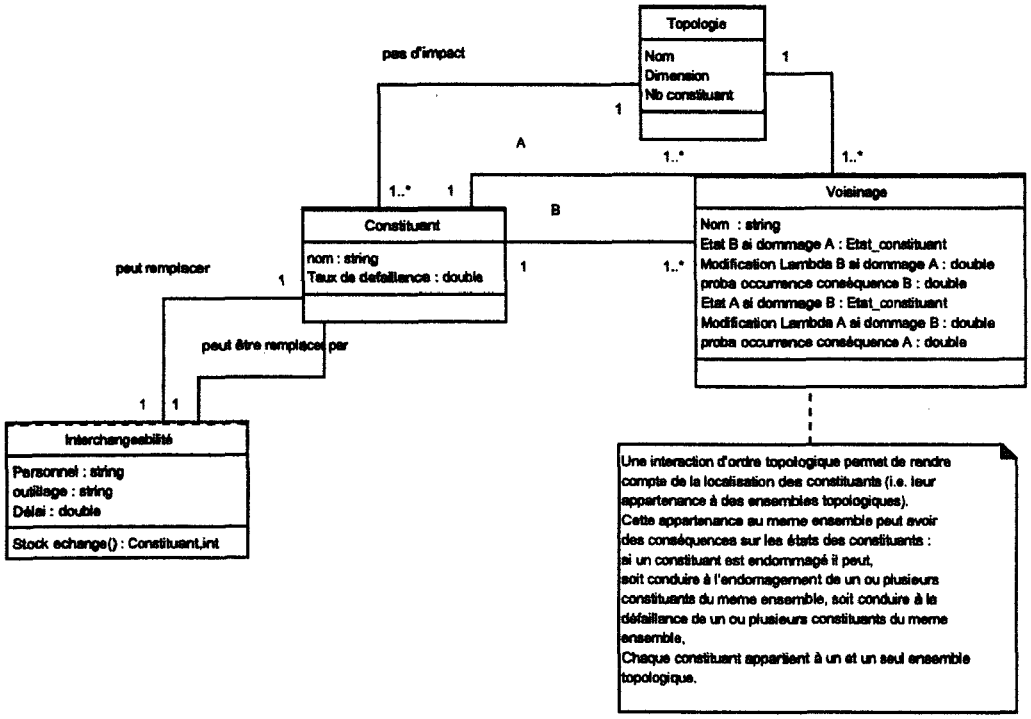

FIG. 3.19 – Diagramme de classe des relations d'interactions entre constituants

tue la base du principe d'agrégation permettant de déterminer l'impact fonctionnel des défaillances d'une part et des dommages d'autre part.

La contribution de la mission aux constituants - relation $R9$

Les relations de contribution de la mission aux constituants permettent de considérer l'impact du contexte opérationnel sur les constituants. Si la fiabilité des systèmes est considérée comme une caractéristique intrinsèque des constituants, la vulnérabilité quant à elle va dépendre du contexte d'exploitation des systèmes. En effet, à chaque séquence sont associées les agressions potentielles qui peuvent survenir. Le diagramme de classe de la figure 3.22 permet de rendre compte de l'impact des agressions sur les constituants par la classe d'association "vulnérabilité". La relation $R9$ est donc définie telle que :

$$R9(a, b) : a \textit{ impact } b \text{ avec,}$$

$a \in A$ (A : ensemble des catégories d'agressions),
$b \in B$ (B : ensemble des constituants).
En d'autres termes, la relation $R9$ permet de considérer les dommages en définissant les constituants qui peuvent être impactés par une catégorie d'agression.

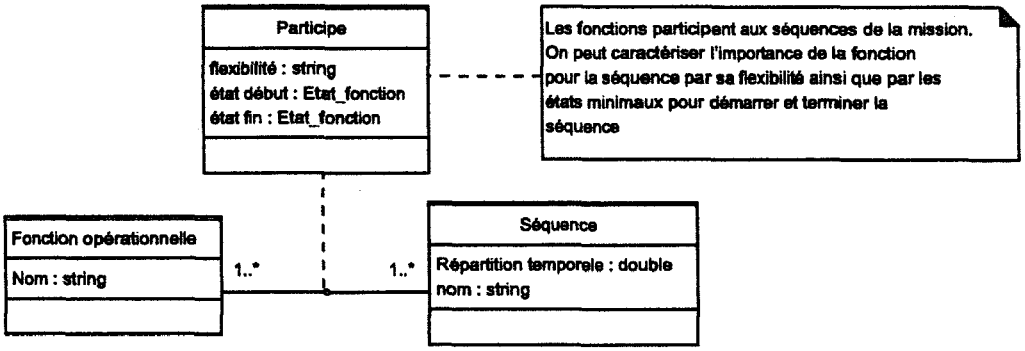

FIG. 3.20 – Diagramme de classe des relations de contribution des fonctions à la mission

Chaque catégorie d'agression est liée aux constituants par le biais de la classe vulnérabilité dans laquelle sont définies les probabilités suivantes (cf. section 3.2.2) :

- la probabilité d'atteindre le constituant,
- la probabilité de détériorer le constituant,
- la probabilité de détruire le constituant.

Ce sont donc ces probabilités (représentatives de la vulnérabilité) qui vont permettre de spécifier le comportement des constituants au regard des agressions et qui permettent d'introduire les dommages subis par les systèmes de manière unifiée avec les défaillances régies quant à elles relativement à la loi de fiabilité des constituants.

Pour terminer la description des systèmes dans le contexte d'une ingénierie de régénération, nous devons introduire dans le modèle structurel les actions de régénération. Sur la base de la représentation de la régénération proposée à la section 3.2.3, nous introduisons un dernier diagramme de classe qui permet de formaliser la description de la régénération sous la forme d'une contribution de la régénération au constituant.

Contribution de la régénération aux constituants - relations $R10$, $R11$ et $R12$

De manière générale, la régénération est caractérisée par le personnel, l'outillage et le délai nécessaire à sa réalisation. La régénération peut être soit un échange ($R10$), soit une réparation ($R11$) ou encore une reconfiguration ($R12$) (cf. section 3.2.3). Pour chaque constituant la possibilité d'échange se matérialise par le stock correspondant, ce stock pouvant provenir du lot de bord, du système de soutien ou d'une interchangeabilité entre composants. On définit donc une relation $R10$ telle que :

$$R10(a, b) : a \textit{ peut être échangé par } b \text{ avec,}$$

$a \neq b \in A^2$ (A : ensemble des constituants).
Pour chaque constituant, la possibilité de réparation est caractérisée par le type de réparation possible (réparation de défaillance ou de dommage), par le nombre de réparations

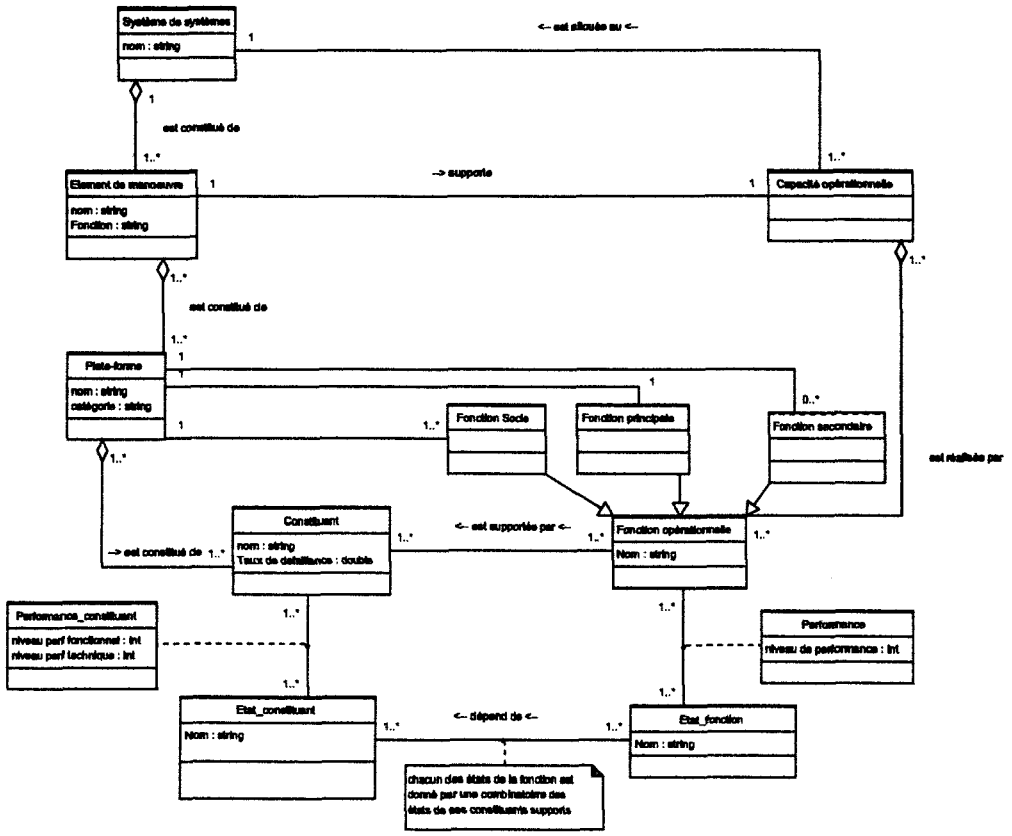

FIG. 3.21 – Diagramme de classe des relations de contribution des constituants aux fonctions

que le composant peut supporter et enfin par les changements d'états correspondants (e.g. détérioré vers régénéré2 dans le cas de la réparation d'un dommage). La réparation est considérée suivant les relations de type $R11$ telles que :

$$R11(a, a) : a \textit{ peut être réparé} \text{ avec,}$$

$a \in A$ (A : ensemble des constituants)

Enfin, la reconfiguration met en jeu 2 constituants, elle peut être de 2 types et peut éventuellement influencer la fiabilité du constituant utilisé en reconfiguration dans la mesure où son utilisation en reconfiguration n'est pas une utilisation normale (attribut "lambda A si A reconfigure B"). Les états des différents constituants après reconfiguration permettent de définir l'impact fonctionnel de la reconfiguration étant donné que l'état des fonctions dépend de l'état de ses constituants supports (cf. diagramme "contribution des constituants aux fonctions" figure 3.21). Les possibilités de reconfiguration sont donc représentées par les relations de type $R12$ avec :

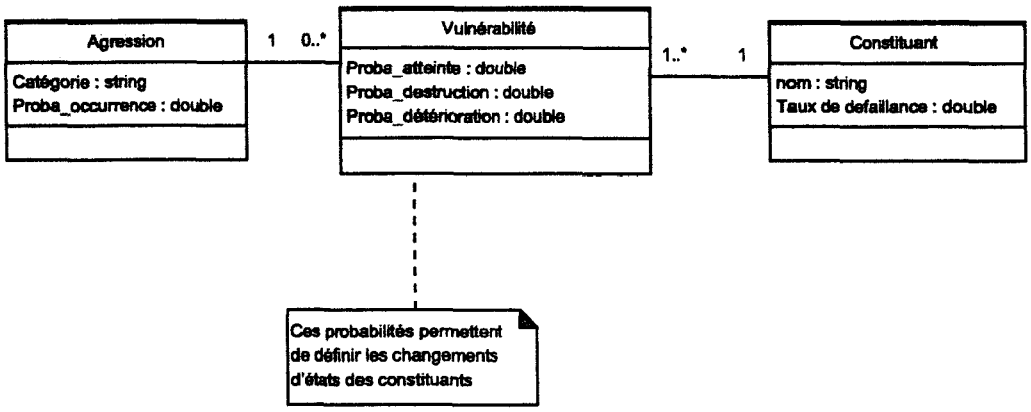

FIG. 3.22 – Diagramme de classe des relations de contribution des agressions aux constituants

$$R12(a, b) : a \textit{ reconfigure } b \text{ avec,}$$

$a \neq b \in A^2$ (A : ensemble des constituants). L'ensemble de ces diagrammes de classe définit donc le modèle de données nécessaire à l'évaluation de la disponibilité opérationnelle en présence de défaillance, de dommage et de régénération. Les diagrammes permettent de définir les différentes dépendances qui interviennent au sein du système et conditionnent ainsi son comportement. Le modèle structurel fournit les éléments à intégrer dans le modèle dynamique. Pour opérer ce passage du modèle structurel au modèle dynamique nous introduisons un ensemble de mécanismes génériques qui permettent de contraindre la construction du modèle dynamique dans le respect de la description du système réalisé dans le modèle structurel. Ces mécanismes permettent notamment de définir formellement le principe d'agrégation qui détermine l'état des fonctions à partir de l'état des constituants et définissent également des dépendances qui permettent de considérer des relations particulières du modèle structurel.

3.4 conclusion

Dans ce chapitre nous avons présenté les fondements de notre contribution méthodologique qui repose sur une approche unifiée de la modélisation des défaillances et des dommages. Nous avons développé l'unification défaillance/dommage sur la base des travaux existants dans la communauté de la SdF pour la représentation des défaillances et dans la communauté de la survivabilité pour la représentation des dommages. La représentation conjointe du comportement d'un composant en présence de défaillances et de dommages nous a ensuite permis d'appréhender le concept de régénération. La même logique d'unification a été appliquée au concept de maintenance et de réparation des dommages subis au combat pour définir la modélisation de la régénération en accord avec la représenta-

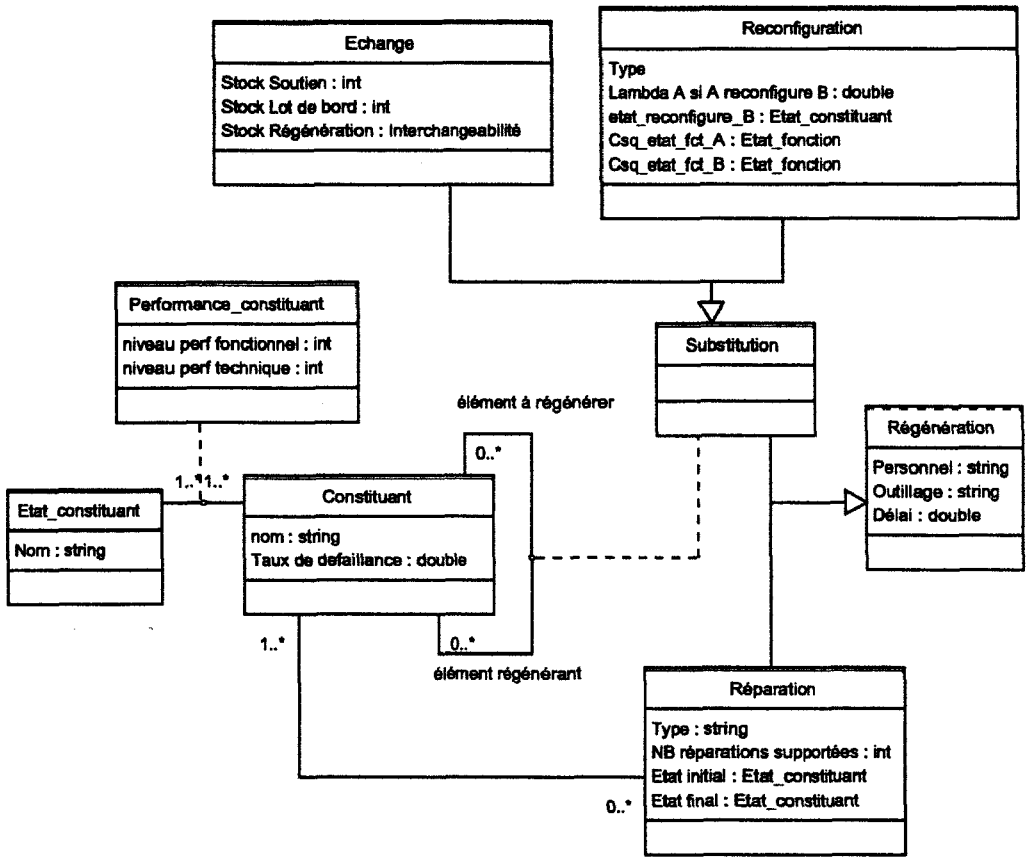

FIG. 3.23 – Diagramme de classe des relations de contribution de la régénération aux constituants

tion des défaillances et des dommages. L'unification défaillance/dommage/régénération nous a donc conduit à la proposition d'un atome de modélisation générique représentatif du comportement des composants en présence de défaillances de dommages et de régénération. Afin de définir une approche aussi générique que possible, nous avons montré comment les fonctions supportées par les composants constitutifs d'un système peuvent être modélisées dans un objectif d'évaluation de la disponibilité opérationnelle. Un atome générique de modélisation des fonctions a donc également été proposé, représentatif des niveaux de performance qui peuvent être associés à une fonction, dans le respect du concept de survivabilité. Ces atomes de modélisation constituent la base de la modélisation des systèmes dont l'objectif est de fournir une représentation des systèmes et de leur comportement qui supporte l'évaluation de la disponibilité opérationnelle. Dans une deuxième partie, nous nous sommes attachés à la formalisation des connaissances nécessaires à la construction de ces atomes de modélisation. Souvent négligée dans la lit-

térature, cette première phase dans une démarche de modélisation constitue souvent une étape délicate dont va dépendre la pertinence des résultats. La méthodologie proposée dans ces travaux repose donc sur une première étape de description des systèmes. Cette description s'appuie sur les principes de la systémique et permet d'intégrer dans le même modèle, le modèle structurel, l'ensemble des éléments qui caractérisent le système dans son contexte opérationnel. La modélisation aborde ainsi le système suivant trois points de vue : organique, fonctionnel et opérationnel. Ces points de vue sont ensuite déclinés suivant trois axes de modélisation : l'axe de décomposition, l'axe d'interaction et l'axe de contribution. Chacun des axes nous permet de définir des relations entre les éléments du même point de vue ou entre points de vue et nous permet de capturer ainsi l'ensemble des relations entre les éléments constitutifs d'un système, définissant ainsi sa *structure*. Pour supporter l'ensemble des relations à la base du modèle structurel et guider la construction d'un modèle structurel particulier, nous avons proposé un ensemble de diagrammes de classe UML qui formalisent l'ensemble des relations définies suivant les axes de modélisation. Afin d'apporter des premiers éléments de validation de la représentation UML du modèle structurel, nous nous sommes basés sur le modèle de données proposé et validé par l'AFIS. Par ailleurs, un autre aspect relatif à la validation du modèle établi dans ces travaux tient à la construction des tables de données dont la structure est donnée par les diagrammes de classe qui permettent de représenter l'ensemble de la connaissance relative au cas d'application défini au chapitre V. La construction d'un modèle structurel particulier (basée sur le principe d'instanciation des diagrammes de classe) nécessite donc de faire appel aux experts des différents domaines concernés (fiabilité, vulnérabilité, soutien logistique, architecture système, ...). Aussi, la définition des classes du modèle structurel basée sur un modèle de données éprouvé en ingénierie système permet aux différents acteurs impliqués dans le modélisation, de manipuler des entités dont le sens est commun à tous.

Dans le chapitre suivant, les relations à la base du modèle structurel nous permettent de définir un ensemble de mécanismes de construction des atomes de modélisation des composants et des fonctions. Ces mécanismes contraignent la construction des atomes et assurent donc une certaine cohérence entre la description du système supportée par le modèle structurel et le modèle dynamique support des évaluations. Nous justifions ensuite l'utilisation du formalisme des Stochastic Activity Networks (SAN) comme support à la construction des atomes de modélisation et à l'évaluation de la disponibilité opérationnelle.

Chapitre 4

Mécanismes de construction des atomes de modélisation supportés par les SANs

Sur la base des relations définies dans le modèle structurel suivant les trois axes de modélisation, des mécanismes de construction ont été définis. Ces mécanismes permettent notamment de définir quels sont les éléments du modèle structurel à prendre en compte dans la définition des conditions de changement d'états dans les atomes de modélisation des constituants et des fonctions. Enfin, pour permettre l'évaluation effective de la disponibilité opérationnelle des systèmes au combat, nous allons porter les atomes de modélisation sur un outil de modélisation et d'évaluation. Le choix de l'utilisation des Stochastic Activity Networks supportés par l'outils Möbius® sera justifié et les modèles correspondant seront présentés.

4.1 Mécanismes génériques de construction du modèle dynamique

Le modèle structurel permet de décrire complètement la structure d'un système dans le sens où, partant des entités qui définissent un système (constituants, fonctions et mission) il permet de définir un ensemble de relations entre ces entités suivant différents axes de modélisation (décomposition, interaction et contribution). Pour évaluer la disponibilité opérationnelle des systèmes, il est nécessaire de construire un modèle dynamique représentatif du comportement du système. Les atomes de modélisation proposés permettent de rendre compte des différents états possibles ainsi que des transitions à considérer entre ces états, indépendamment de tout formalisme de modélisation. L'objectif des mécanismes de construction proposés dans la suite est donc de contraindre la construction des modèles dynamiques en spécifiant tout ou partie des éléments intervenant dans les transitions entre les différents états des composants et des fonctions, sur la base des relations d'interactions et de contributions identifiées dans le modèle structurel. Pour être générique, ces mécanismes basés sur les relations $R4$ à $R12$ et les atomes de modélisation des constituants et des fonctions, sont exprimés indépendamment du formalisme support des modèles dynamiques. Ces mécanismes ont donc pour objectif de guider la construction des atomes de modélisation et plus particulièrement, de définir les éléments à considérer dans la définition des transitions en fonction de la connaissance disponible dans le modèle structurel. Ainsi, ajoutés au modèle structurel, ces mécanismes de construction réduiront la difficulté de construction du modèle dynamique suivant le formalisme adapté.

4.1.1 Notations

Pour définir les mécanismes de construction, nous introduisons tout d'abord un ensemble de notations (table 4.1) nous permettant de manipuler les éléments du modèle structurel. Ces mécanismes contraignent le modèle des constituants et le modèle des fonctions en définissant notamment les éléments qui interviennent sur les conditions de changement d'états. Ces conditions seront exprimées par le biais de relations notées $\mathscr{R}_i$, fonctions d'un ensemble de paramètres tels que :

$$T(X_i^a, X_j^a) = \mathscr{R}_i(P_1, ..., P_n), \text{ avec}$$

$T(X_i^a, X_j^a)$ la transition de l'état X_i^a vers l'état X_j^a où $X \in E$ *ou* e et
$(P_1, ..., P_n)$ un ensemble de paramètres.
Les relations identifiées dans le modèle structurel vont donc nous permettre de préciser l'ensemble de paramètres conditionnant des transitions particulières.

TAB. 4.1 – Notations

F={fonctions opérationnelles}	*ensemble des fonctions opérationnelles*
C={Constituants}	*ensemble des constituants*
E={états des fonctions}	*ensemble des états des fonctions*
e={états des constituants}	*ensemble des états des constituants*
A={Agressions}	*ensemble des catégories d'agressions*
E_i^a	*état i de la fonction a*, avec $E_i^a \in$ E, $1 \leq i \leq 4$, cf. figure 3.4 et $a \in$ F
e_i^a	*état i du constituant a*, avec $e_i^a \in$ e, $1 \leq i \leq 7$, cf. figure 3.5 et $a \in$ C
$T(E_i^a, E_j^a)$	*Transition de l'état E_i de la fonction a vers l'état E_j de la fonction a*
$T(e_i^a, e_j^a)$	*Transition de l'état e_i du constituant a vers l'état e_j du constituant*
x.a	*attribut "a" de l'élément x, avec $x \in classeX$*
x.y.a	*attribut "a" de l'élément y, en relation avec l'élément x avec $y \in classeY$ et $x \in classeX$*

4.1.2 Les mécanismes de construction de l'atome de modélisation des constituants

Sur la base des notations proposées ci-avant, les mécanismes de construction des modèles dynamiques de constituants sont détaillés. Les différents mécanismes sont présentés relativement aux relations du modèle structurel à partir desquelles ils sont construits.

Mécanismes basés sur les interactions entre constituants

Deux relations d'interaction entre les composants ont été identifiées dans le modèle structurel. Chacune de ces relations va donc conduire à un mécanisme de construction représenté par une relation $\mathscr{R}_i$. Le premier mécanisme, dérivé des relations d'interaction s'applique dans le cadre d'une relation d'interchangeabilité $R5(a,b)$, avec $(a,b) \in C$:
si $\exists\ a, b \in C$ *tel que* $R5(a,b)$ alors $\exists\ (i) \in [1,7]$
$T(e^a_{panne}, e^a_{ok}) = \mathscr{R}_1(e^b_i, P)$
$T(e^b_{panne}, e^b_{ok}) = \mathscr{R}_2(e^a_i, P)$

avec P ensemble des autres paramètres de T[1].
On exprime ainsi une contrainte sur le paramétrage d'une transition relative à un échange du constituant telle que cette transition sera possible par interchangeabilité moyennant

[1]Cette notation sera conservée pour l'ensemble des mécanismes présentés.

un état particulier e_i^b du constituant qui va remplacer le constituant en panne.

La topologie du système (i.e. la localisation des différents constituants) considérée dans la modélisation au travers des relations d'interactions $R6(a,b)$ permet également de définir un mécanisme de construction au niveau du modèle dynamique des constituants. En particulier, la prise en compte de la topologie permet de modéliser la propagation des dommages d'un constituant vers un autre avec pour conséquence l'endommagement, la défaillance ou une modification de la fiabilité du constituant non directement atteint. Ainsi, relativement au diagramme de classe de la figure 3.19, la relation $\mathscr{R}_3$ est telle que :
si $\exists\ a, b \in C$ *tel que* $R6(a,b)$
et $b.Voisinage.probabilite\_occurrence\_consequenceB \neq 0$ *alors*,
$\exists\ e_i^a \in \{deteriore, detruit\}$
$\exists\ e_k^b \in \{deteriore, detruit, panne\}$
$\exists\ (j) \in [1,7]$
$T(e_j^b, e_k^b) = \mathscr{R}_3(e_i^a, b.Voisinage.probabilite\_occurrence\_consequenceB, P)$

Cette écriture permet donc de considérer la propagation des dommages entre les constituants en fonction de leur localisation dans le système.

Mécanismes basés sur les relations de contribution de la mission aux constituants

Les relations $R9$ permettent de mettre en relation les catégories d'agressions considérées pour la mission avec les constituants susceptibles d'être impactés. Ces relations du modèle structurel vont donc permettre de définir les transitions des constituants vers les états relatifs aux dommages ({détérioré,détruit}). Ces transitions dépendent notamment des attributs de vulnérabilité des constituants qui interviennent dans les relations $\mathscr{R}_4$ et $\mathscr{R}_5$ telles que :
si $\exists\ a \in A$ *et* $b \in C$ *tel que* $R9(a,b)$ *alors*
$\exists\ (i) \in [1,7]$
$T(e_i^b, e_{deteriore}^b) = \mathscr{R}_4(vulnerabilite.prob\_atteinte, vulnerabilite.prob\_deteriore, P)$
$T'(e_i^b, e_{detruit}^b) = \mathscr{R}_5(vulnerabilite.prob\_atteinte, vulnerabilite.prob\_detruit, P)$

où, $vulnerabilite.prob\_atteint$, $vulnerabilite.prob\_deteriore$ et $vulnerabilite.prob\_detruit$ données de vulnérabilité du constituant b pour la catégorie d'agression a.

Mécanismes liés à la régénération

Les derniers mécanismes qu'il est possible de définir au niveau des constituants seront pris en considération au moyen des relations de contribution de la régénération aux constituants. La modélisation de la régénération dans le modèle structurel est réalisée par trois relations de contributions différentes, relatives chacune à un type de régénération particulier. La première relation de contribution de la régénération aux constituants est la relation $R10(a,b)$ qui définit une opération d'échange entre les constituants a et b avec $a, b \in C$. Par ailleurs au niveau du constituant, nous avons déjà défini les relations

$\mathscr{R}_1$ et $\mathscr{R}_2$ relatives au mécanisme de construction induit par la présence d'une interchangeabilité. Ainsi, la relation $R10(a,b)$ va nous permettre d'affiner les relations $\mathscr{R}_1$ et $\mathscr{R}_2$ en apportant de nouveaux éléments relatifs aux transitions. Nous définissons donc deux nouvelles relations $\mathscr{R}_6$ et $\mathscr{R}_7$ telles que :

si $\exists$ a *et* $b \in C^2$ *tel que* $R10(a,b)$ alors
$\exists\ i,j\ \in [1,7]^2$
$T(e^a_{panne}, e^a_{ok}) =$
$\mathscr{R}_6(e^b_i, b.echange.stock\_Soutien, b.echange.stock\_lot\_bord, b.stock\_regeneration, P)$
$T'(e^b_{panne}, e^b_{ok}) =$
$\mathscr{R}_7(e^a_j, a.echange.stock\_Soutien, a.echange.stock\_lot\_bord, a.stock\_regeneration, P)$

Le deuxième mécanisme permettant de considérer la régénération dans le modèle dynamique s'attache donc à préciser les transitions relatives aux réparations sur la base des relations $R11$. On obtient la relation $\mathscr{R}_8$ suivante :

si $\exists$ $a \in C$ *tel que* $R11(a,a)$ alors
$\exists\ (i) \in [1,7]$ *tel que* $e^a_i = a.reparation.Etat\_initial$
$\exists\ (j) \in [1,7]$ *tel que* $e^a_i = a.reparation.Etat\_final$
$T(e^a_i, e^a_j) = \mathscr{R}_8(a.reparation.type, a.NB\_reparations\_suportees, a.regeneration.delai, P)$

Cette relation $\mathscr{R}_8$ générique permet de représenter les éléments à considérer dans le cas d'une réparation de défaillance ($a.reparation.type = defaillance$) ou dans le cas d'une réparation de dommage ($a.reparation.type = dommage$). Chaque attribut est alors clairement spécifié et permet de déterminer la transition concernée. On aura par exemple dans le cas de la réparation d'un dommage :

- $a.reparation.type = dommage$,
- $a.reparation.Etat\_initial = deteriore$,
- $a.reparation.Etat\_final = regenere2$,

la transition concernée est alors : $T(e^a_{deteriore}, e^a_{regenere2})$.

Le dernier mécanisme de construction dérivé des relations de contribution de la régénération aux constituants relève des actions de reconfiguration relatives aux relations de type $R12(a,b)$ avec $a,\ b\ \in\ C^2$. Cette relation permet de définir tout d'abord un mécanisme spécifiant la transition vers l'état "panne" du constituant a correspondant à l'impact de la reconfiguration sur la fiabilité. Nous introduisons donc la relation $\mathscr{R}_9$ telle que :

si $\exists$ $a,b \in C^2$ *tel que* $R12(a,b)$ alors
$\exists$ $Lamdba\_a$ *tel que* $Lamdba\_a = a.reconfiguration.Lamdba\_a\_si\_a\_reconfigure\_b$
$T(e^a_{en\_reconfiguration}, e^a_{panne}) = \mathscr{R}_9(Lambda\_a, P)$

Ensuite, un mécanisme précise l'action de reconfiguration en déterminant l'état du composant a après l'action de reconfiguration. Cette transition dépend donc de l'état du composant b qui conduit à la mise en oeuvre de l'action de reconfiguration. On définit donc la relation $\mathscr{R}_{10}$ telle que :

si $\exists$ $a,b \in C^2$ *tel que* $R12(a,b)$ *alors*
$\exists\ (i) \in [1,7]$ *tel que* $e^b_i = a.reconfiguration.etat\_reconfiguré\_B$
$T(e^a_{ok}, e^a_{en\_reconfiguration}) = \mathscr{R}_{10}(e^b_i, a.regeneration.delai, P)$

4.1.3 Les mécanismes de construction de l'atome de modélisation des fonctions

Comme pour l'atome de modélisation des constituants, on peut, à partir des relations du modèle structurel, définir des mécanismes de construction pour les atomes de modélisation des fonctions.

Mécanismes basés sur les interactions fonctionnelles

Le premier mécanisme identifié est dérivé des relations d'interaction entre les fonctions. En effet, une relation d'interaction $R4(a,b)$ entre deux fonctions a et b implique qu'il existe une dépendance entre ces deux fonctions. Cette dépendance se matérialise au niveau du modèle dynamique entre les états des fonctions concernées : une ou plusieurs transition(s) entre les états de b va(vont) dépendre d'un ou plusieurs état(s) de a. On obtient donc la relation $\mathscr{R}_{11}$ telle que :
si $\exists\ a,b \in F^2$ *tel que* $R4(a,b)$ alors
$\exists\ (i,j) \in [1,4]^2$
$\exists\ k \in [1,4]$
$T(E_i^b, E_j^b) = \mathscr{R}_{11}(E_k^a, P)$

Mécanisme basé sur la contribution des constituants aux fonctions : les règles d'agrégation

Les relations de type $R8(a,b)$ avec $a \in C$ et $b \in F$ vont nous permettre de définir les règles d'agrégation qui déterminent l'état d'une fonction à partir de la connaissance de l'état des constituants qui la supportent. Ces règles d'agrégation sont construites sur le même principe que le modèle de liaison réseau de Petri défini par Betous-Almeida (C. Betous-Almeida 2002). Dans ces travaux, la structure du modèle de liaison définit les conditions sur les états des composants qui déterminent les changement d'état des fonctions. De manière à nous affranchir dans un premier temps de tout formalisme support du modèle dynamique, nous appellerons *règle d'agrégation* les conditions sur les états des constituants qui définissent les changements d'état des fonctions. L'état d'une fonction va donc être obtenu par la connaissance des règles d'agrégation qui la concernent et de la relation $\mathscr{R}_{12}$ si elle existe. Le mécanisme basé sur cette relation impose donc de prendre en compte les états des constituants support de la fonction dans la définition des transitions entre les états de la fonction. Ce mécanisme est défini comme suit :
soit n le nombre de constituants support de la fonction f *avec* $f \in F$ alors
$\exists\ 1 \leq i \leq n$ *tel que* $R8(a(i), f)$, *avec* $a(i) \in C$
$\exists\ k \in [1,7]$ *tel que* $e_k^i \in e$
$\exists\ (l,m) \in [1,4]^2$
$T(E_l^f, E_m^f) = \mathscr{R}_{12}(e_1^1, ..., e_7^1, ..., e_k^i, ..., e_1^n, ..., e_7^n, P)$

Ce mécanisme impose donc de considérer l'ensemble des états des constituants dans la définition de chacune des transitions de la fonction supportée par cet ensemble de constituants.

Mécanismes basés sur la contribution de la régénération aux constituants

Parmi les actions de régénération, une action de reconfiguration peut mettre en oeuvre deux constituants qui ne supportent pas la même fonction. Elle a donc un impact sur ces fonctions qui conduit à la définition de deux mécanismes supplémentaires relatifs à la construction de l'atome de modélisation des fonctions. Ces mécanismes supportés par les relations $\mathscr{R}_{13}$ et $\mathscr{R}_{14}$ sont définis comme suit :

si $\exists\ a, b \in C^2$ *et* $f1, f2 \in F^2$ *tels que* $R12(a,b)$ et $R8(a,f1)$ et $R8(b,f2)$ alors

$\exists\ i,j,k,l \in [1,4]^4$ tels que

$E_j^{f1} = a.regeneration.Csq\_etat\_fct\_A$

$E_k^{f1} \neq OK$

$E_l^{f2} = a.regeneration.Csq\_etat\_fct\_B$

$T(E_i^{f1}, E_j^{f1}) = \mathscr{R}_{13}(e^a_{en\_reconfiguration}, P)$

$T(E_k^{f2}, E_l^{f2}) = \mathscr{R}_{14}(e^a_{en\_reconfiguration}, P)$

Ces deux mécanismes viennent donc en complément du mécanisme supporté par la relation $\mathscr{R}_{12}$ et devront être considérés simultanément avec ce dernier dans la construction des modèles des fonctions.

4.1.4 Conclusion

Nous avons présenté les deux premières étapes de notre démarche de modélisation proposée au travers de la description du modèle structurel et du modèle dynamique. Basé sur la démarche d'ingénierie système, le modèle structurel permet de structurer la connaissance indispensable à l'évaluation de la disponibilité. Il intègre les aspects fonctionnel, technique et opérationnel d'une architecture ainsi que les relations de dépendances et d'interactions. A partir des relations à la base du modèle structurel, des règles de construction des atomes de modélisation du comportement des constituants et des fonctions ont été définies. Ces règles permettent de contraindre la spécialisation des atomes en fonction des éléments contenus dans le modèle structurel. Ces règles assurent tout ou partie de la cohérence entre la description du système réalisée dans le modèle statique, avec le modèle dynamique des constituants et des fonctions qui en découlent.

4.2 Le modèle dynamique du comportement des systèmes

Dans la section précédente, nous avons présenté des mécanismes génériques de construction des atomes de modélisation des constituants et des fonctions. Ces mécanismes permettent de définir tout ou partie des transitions entre les états d'un constituant ou d'une fonction sur la base des connaissances sur le système formalisées dans le modèle structurel. Ces mécanismes génériques ont été définis indépendamment du formalisme choisi pour supporter le modèle dynamique. Pour évaluer quantitativement la disponibilité opérationnelle des systèmes, le modèle dynamique sous sa forme conceptuelle doit être porté par un formalisme de modélisation. Couplé à une technique d'évaluation, il per-

mettra d'analyser le comportement dynamique des systèmes en présence de défaillances, de dommages et de régénération.

4.2.1 Choix du formalisme support du modèle dynamique

Le modèle dynamique résulte, d'une part, de la construction des différents modèles atomiques relatifs aux constituants et aux fonctions, et d'autre part, de la mise en relation des modèles atomiques dans le respect des mécanismes de construction dérivés du modèle structurel. Le formalisme de représentation adopté doit donc être capable d'intégrer à la fois la structure du système telle qu'elle est définie dans le modèle structurel et les processus stochastiques régissant la dynamique du système. De plus, il est préférable de disposer d'une méthode (et/ou un outil) de calcul couplée au formalisme afin d'analyser le comportement dynamique du système. Aussi, relativement aux conclusions du chapitre II, les principales techniques de modélisation pour l'évaluation quantitative de la sûreté de fonctionnement et, plus particulièrement, l'évaluation de la disponibilité sont les suivantes, (K.S. Trivedi et M. Malhotra 1993) :

- les Chaînes de Markov,
- les réseaux de Petri Stochastiques et leurs différentes extensions.

Relativement à la représentation des défaillances, des dommages et de la régénération définie au chapitre 3, la technique de modélisation devra répondre aux critères suivants :

1. autoriser la représentation de processus stochastiques régis par des distributions de probabilités générales (exponentielle, discrète, lognormale,...),
2. permettre la prise en compte des interactions entre les constituants et entre les fonctions (transitions fonction de l'état courant dans un autre modèle),
3. permettre la modélisation des règles d'agrégation déterminant l'état des fonctions, à partir de l'état de leurs constituants supports.
4. respecter la décomposition hiérarchique des systèmes par une modélisation modulaire et hiérarchique.

Les chaînes de Markov, bien que largement utilisées dans les études de sûreté de fonctionnement pour leurs capacités à fournir des évaluation exactes, souffrent cependant de limitations difficilement contournables face à la problématique de la régénération. On trouve notamment différentes techniques qui autorisent une approche analytique dans les cas où l'hypothèse markovienne n'est plus respectée. On peut citer :

- la méthode des états fictifs,
- la méthodes des variables complémentaires.

Une illustration de ces techniques est donnée dans (J. Muppala, R. Fricks et K. Trivedi 2000). Les auteurs ont également travaillé à la représentation de dépendances dans la modélisation markovienne pour la sûreté de fonctionnement (J. Muppala et K. Trivedi 1995). Il est notamment montré comment les dépendances en terme d'action de maintenance peuvent être représentées dans une chaîne de Markov. Les chaînes de Markov restent donc une technique privilégiée en sûreté de fonctionnement. De plus, différentes techniques ont été développées pour traiter, à partir d'une chaîne de Markov, des processus non Markoviens ou des dépendances au sein d'un système. Cependant, elles augmentent

notoirement la complexité des modèles et trouvent rapidement leurs limites dans le cas de grands systèmes. A cela s'ajoute le problème d'explosion combinatoire qui rend la conception et la lecture des modèles fastidieuses et constitue ainsi une source d'erreur. Pour réaliser les études de sûreté de fonctionnement, l'extension la plus couramment utilisée correspond aux réseaux de Petri stochastiques Généralisés (M. Malhotra et K. Trivedi 1995, R.M. Fricks et K.S. Trivedi 1997, C. Betous-Almeida 2002). Ils présentent plusieurs avantages au regard des chaînes de Markov, les plus significatifs étant, (J-F Ereau 1997) :

- la maîtrise de l'explosion combinatoire,
- le pouvoir de modélisation,
- des possibilités de vérification formelle,
- l'intelligibilité des modèles,
- la possibilité de résolution analytique par construction de la chaîne de Markov équivalente aux graphes de marquage,
- la mise en oeuvre efficace de leur simulation.

Les réseaux de Petri offrent en effet la possibilité de construire des modèles intelligibles plus compacts qu'une chaîne de Markov et réduisant le phénomène d'explosion combinatoire du nombre d'états. Par ailleurs, ils supportent également la résolution analytique dans le cas où l'hypothèse markovienne est respectée et des extensions ont également été apportées pour traiter des systèmes non markoviens (Ricardo Fricks et al. 1998). Cependant, les réseaux de Petri deviennent difficiles à manipuler dans le cas de grands systèmes dans lesquels les dépendances sont nombreuses. Plus particulièrement, la notion d'agrégation proposée conduirait à une construction délicate des réseaux en raison du combinatoire entre les états des composants. Une extension particulièrement intéressante introduite par Cardio *et. al.*, (G. Ciardo, J.K. Muppala et K.S. Trivedi 1992) et illustrée par Malhotra et Trivedi (M. Malhotra et K. Trivedi 1995) repose sur la définition de variables de récompense définissant ainsi les *Stochastic Reward Nets (SRN)*. Les SRN permettent de simplifier la construction du modèle et en réduisent considérablement la taille en définissant des variables de récompense représentatives des performances de sûreté de fonctionnement qui permettent l'évaluation de taux de récompense dépendant du marquage des réseaux. Des aspects qui seraient explicitement modélisés par des places et des arcs dans un réseau de Petri stochastique généralisé se trouvent dans un SRN exprimés sous la forme d'une équation arithmétique et/ou booléenne du taux de récompense. Permettant ainsi une approche de modélisation plus générique et modulaire, les SRN supportent également une résolution analytique par construction de la chaîne de markov équivalente définissant ainsi un Markov Reward Model (cf. figure 2.2 au chapitre 2). Dans le cas de grands systèmes complexes pour lesquels la simulation devient incontournable (K. Upadhya et N. Srinivasan 2005), les réseaux de Petri stochastiques restent une technique de modélisation privilégiée qui bénéficie d'un pouvoir de modélisation étendu et qui constitue un bon support aux simulations (J-F Ereau 1997, Y. Dutuit et al. 1997, J.L. Chabot, Y. Dutuit et A. Rauzy 2001). Parmi les extensions des RdP supports aux simulations, les Stochastic Activity Networks allient la puissance des SRN dans la construction et l'expressivité des modèles par l'utilisation de variables récompenses avec la puissance de résolution offerte par les simulations. De plus, le formalisme

des *portes* fournit une très grande souplesse dans la modélisation de comportements complexes et facilite la prise en compte de dépendances à partir d'équations combinatoires sur le marquage des états du réseaux. Les *portes* lèvent donc le principal inconvénient identifié pour les réseaux de Petri. Ces possibilités étendues de modélisation peuvent cependant être source d'erreurs et justifient l'étape de formalisation des connaissances et la définition de mécanismes de construction.

Particulièrement adaptés au études de sûreté de fonctionnement dans un contexte d'ingénierie système (S.T. Beaudet, T. Courtney et W. Sanders 2006), les SANs ont donc été retenus pour supporter le modèle dynamique constitué d'un ensemble d'atomes de modélisation des constituants et des fonctions, construits dans le respect des règles précédemment définies à la section 4.1. Nous allons donc dans la suite illustrer l'utilisation des SANs comme supports aux atomes de modélisation des constituants et des fonctions.

4.2.2 Application des mécanismes de construction du modèle pour l'obtention du modèle SANs

Définition d'un Stochastic Activity Network

Avant d'aborder concrètement la construction des atomes de modélisation, nous allons rappeler brièvement les fondements des Stochastic Activity Networks. Les définitions présentées ci-après sont extraites des travaux de Sanders et Meyer (W.H. Sanders et J.F. Meyer 2001). Comme les Réseaux de Petri stochastiques ont été définis à partir des réseaux de Petri "classiques", les Stochastic Activity Networks sont définis à partir des Activity Networks.

Définition 4.1 (Activity Network). *Un Activity Network (AN) est un 8-uplet*

$$AN = (P, A, I, O, \gamma, \tau, \iota, o)$$

où, P est un ensemble fini de places,
A est un ensemble fini d'activités,
*I est un ensemble fini d'*input gate,
*O est un ensemble fini d'*output gate,
$\gamma : A \rightarrow \mathbb{N}^+$ spécifie le nombre de cas de chaque activité, et
$\tau : A \rightarrow \{Temporisée, Instantanée\}$ spécifie le type de chaque activité.
La structure du réseau est spécifiée à l'aide des fonctions ι et o :
$\iota : I \rightarrow A$ met en relation les input gates *aux activités, tandis que*
$o : O \rightarrow \{(a, c) | a \in A$ et $c \in \{1, 2, ..., \gamma(a)\}\}$ met en relation les output gates *aux cas des activités.*

Nous pouvons maintenant préciser les notions de marquage, *input gate* et *output gate* avant de donner la définition d'un SAN. Soit P l'ensemble de toutes les places du réseau.

Si S est un ensemble de places tel que ($S \subseteq P$) *un marquage de* S est une fonction $\mu : S \rightarrow \mathbb{N}$. De la même manière, l'ensemble des *marquages possibles de* S est un ensemble de fonctions $M_S = \{\mu \mid \mu : S \rightarrow \mathbb{N}\}$. Une *input gate* peut maintenant être définie comme un triplet, (G, e, f), où ($G \subseteq P$) est l'ensemble des places d'entrées de la porte, $e : M_G \rightarrow \{0,1\}$ définie la condition d'activation de la porte et $f : M_G \rightarrow M_G$ est la fonction d'entrée de la porte. De la même façon une *output gate* est définie comme le couple (G, f), où ($G \subseteq P$) est l'ensemble des *places de sorties* associées à la porte et $f : M_G \rightarrow M_G$ constitue le fonction de sortie de la porte.

Étant donné un activity network, et les notations introduites ci-dessus, un stochastic activity network est formé en ajoutant les fonctions C, F et G où, C spécifie la distribution de probabilité de sélection des cas, F représente les fonctions de distribution de probabilité des délais associés aux activités et G décrit les ensembles de "marquages de réactivation" pour chaque marquage possible.

Définition 4.2 (Stochastic Activity Network). *Un Stochastic Activity Network* (SAN) *est un quintuplet*

$$SAN = (AN, \mu_0, C, F, G)$$

où,

$AN = (P, A, I, O, \gamma, \tau, \iota, o)$ *est un activity network*

$\mu_0 \in M_P$ *est un marquage initial,*

C est l'attribution de distribution de cas, une attribution de fonctions aux activités telle que pour n'importe quelle activité a, $C_a : M_{IP(a) \cup OP(a)} \times \{1, ..., \gamma(a)\} \rightarrow [0,1]$. De plus, étant donnée une activité a et un marquage $\mu \in M_{IP(a) \cup OP(a)}$ dans lequel a est valide, $C_a(\mu, \cdot)$ est une distribution de probabilité appelée "distribution des cas de a dans μ".

F définit la densité de probabilité de durée de l'activité, F associe des fonctions continues aux activités temporisées telles que pour toute activité a, $F_a : M_P \times \mathbb{R} \rightarrow [0,1]$. De plus, étant donné un marquage stable $\mu \in M_P$ et une activité temporisée a valide pour μ, $F_a(\mu, \cdot)$ est une densité de probabilité continue appelée "densité de probabilité de la durée de l'activité a pour le marquage μ ; avec $F_a(\mu, \tau) = 0$ si $\tau \leq 0$".

G définit la fonction de réactivation : association de fonctions aux activités temporisées telles que pour toute activité a, $G_a : M_P \rightarrow \wp(M_P)$, où $\wp(M_P)$ dénote l'ensemble des parties de M_P. De plus, pour tout marquage stable $\mu \in M_P$ et pour toute activité

temporisée a valide pour μ, $G_a(\mu, \cdot)$ est un ensemble de marquages appelés marquages de réactivation de a pour μ.

De plus, comme les réseaux de Petri, les SANs offrent le confort d'une modélisation graphique permettant de construire les modèles sur la base des représentations graphiques de ses éléments constitutifs : les places, les *input gates*, *output gates*, les transitions instantanées et les transitions temporisées. Ces éléments sont représentés dans la figure 4.1.

FIG. 4.1 – Représentation graphique des éléments d'un SAN

Nous avons donné la définition formelle des SAN sur la base de la définition proposée par Sanders, (W.H. Sanders et J.F. Meyer 2001), nous invitons le lecteur à se reporter aux travaux de (W. Sanders 1988, A. Movaghar n.d., W.H. Sanders et J.F. Meyer 2001), pour plus de précisions. Sur la base de ces définitions, nous illustrerons dans la suite la flexibilité de modélisation qu'offrent les SAN à travers la présentation de la construction des atomes de modélisation des constituants et des fonctions. Plus particulièrement, nous verrons comment les fonctions de marquages définies dans les *output gates* et la possibilité de définir des distributions de probabilités fonction du marquage nous permettent de respecter l'ensemble des mécanismes de construction proposé dans la section précédente.

Définition des variables de récompense

Sur la base de la structure du réseau défini et du comportement spécifié, l'évaluation du modèle SAN construit nécessite la définition de variables de récompense qui donnent accès aux mesures attendues. Pour donner la définition des variables de récompense associées aux SANs, nous présentons la définition de la *structure de récompense basée sur les activités et le marquage* d'un SAN, proposée par Sanders (W. Sanders 1988) :

Définition 4.3. *La structure de récompense d'un SAN avec P l'ensemble des places et A l'ensemble des activités est toute paire de fonctions $(\mathscr{C}, \mathscr{R})$, avec :*
$\mathscr{C} : A \rightarrow \mathbb{R}$ *où, pour $a \in A$, $\mathscr{C}(a)$ est la récompense obtenue après la réalisation de l'activité a, et*
$\mathscr{R} : \mathscr{P}(P, \mathbb{N}) \rightarrow \mathbb{R}$, *où pour $\nu \in \mathscr{P}(P, \mathbb{N})$, $\mathscr{R}(\nu)$ est le taux de récompense obtenu quand pour chaque $(p, n) \in \nu$, il y a n jetons dans la place p,*

où $\mathbb{N}$ est l'ensemble des entiers naturels et $\mathscr{P}(P, \mathbb{N})$ est l'ensemble des fonctions partielles entre P et $\mathbb{N}$, telles que $\nu \in \mathscr{P}(P, \mathbb{N})$ constitue un marquage partiel[2]. L'association de variables de récompense avec les modèles SANs des constituants et des fonctions vont ainsi nous permettre de définir des variables de performance avec une grande souplesse dans le choix des grandeurs à évaluer.

Modèle SAN de l'atome de modélisation des constituants

L'interprétation des mécanismes de construction décrits indépendamment de tout formalisme support de l'atome de modélisation va donc nécessairement dépendre du formalisme choisi et de la logique de modélisation adoptée. Ainsi, nous présentons dans cette partie, comment l'atome conceptuel de modélisation du comportement des constituants peut être porté par le formalisme des SANs dans le respect des mécanismes de construction. Chacun des aspects des atomes de modélisation peut être décrit dans le formalisme des SANs qui n'induit donc pas de perte sémantique. Nous commençons tout d'abord par rappeler l'atome conceptuel de modélisation à la figure 4.2. Cette représentation

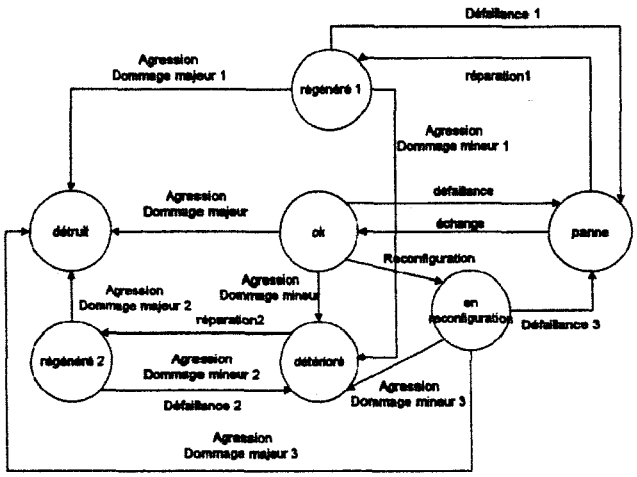

FIG. 4.2 – Représentation du comportement en présence de défaillances, de dommages et de régénération

nous sert de base pour représenter la structure du modèle atomique dans le formalisme des SAN qui intègre les mécanismes de construction. Le premier mécanisme considéré pour la construction du modèle repose sur les relations $\mathscr{R}_4$ et $\mathscr{R}_5$, qui permettent de rendre compte des dommages en considérant les transitions vers les états *détérioré* et *détruit*. Cette transition dépend de la probabilité d'être atteint qui est propre au constituant pour chaque catégorie d'agression considérée. Nous proposons donc d'ajouter aux

[2]Le marquage est partiel dans le sens où des entiers naturels sont associés à des sous-ensembles de P ; un marquage sera "total" si des entiers naturels sont associés à toutes les places de l'ensemble P

places représentant l'ensemble des états *{ok, panne, détérioré, détruit, régénéré1, régénéré2, en_reconfiguration}*, une place représentant l'agression. Le marquage de cette place représente la catégorie d'agression et évolue donc en fonction de l'occurrence de la catégorie d'agression et de la probabilité pour le constituant d'être atteint par cette catégorie. Ensuite, étant donnée la possibilité dans les SAN de définir des "cas" au niveau des activités, l'agression au niveau du constituant sera représentée par une activité avec deux cas : le premier conduisant dans l'état *détérioré* et le second conduisant dans l'état *détruit*. Ainsi, pour chaque catégorie d'agression susceptible d'atteindre le constituant, les probabilités d'être détruit et détérioré intervenant dans les relations $\mathscr{R}_4$ et $\mathscr{R}_5$ (vulnerabilite.proba_deteriore et vulnerabilite.proba_detruit) définissent la distribution de probabilité des cas de la transition de telle sorte que pour chaque catégorie d'agression :

$$(vulnerabilite.proba\_deteriore + vulnerabilite.proba\_detruit) = 1$$

La condition de validation de cette activité sera donc fonction du marquage de la place *agression* et du marquage des places représentant les états dans lesquels le constituant peut subir une agression : $G = \{ok, régénéré1, régénéré2, en\_reconfiguration, agression\}$, avec $G \subseteq P$ et
$P = \{ok, panne, détérioré, détruit, régénéré1, régénéré2, en\_reconfiguration, agression\}$
que nous représenterons par une place *e_i* pour l'exemple. Conformément à la définition des SANs, cette condition constituera la fonction $e : M_G \rightarrow \{0,1\}$ d'activation de la porte. On aura par exemple une fonction e telle que :
$e = ((\mathscr{M}_{ok} = 1 \vee \mathscr{M}_{régénéré1} = 1 \vee \mathscr{M}_{régénéré2} = 1 \vee \mathscr{M}_{en\_reconfiguration} = 1) \wedge \mathscr{M}_{agression} \neq 0)$
où, $\mathscr{M}_X$ représente le marquage de la place X, $\vee$ correspond à l'opérateur booléen "OU" et $\wedge$ à l'opérateur "ET". Il reste maintenant à définir l'évolution du marquage une fois l'activité terminée. On introduira donc une *output gate* du cas 1 vers l'état *détérioré* et une autre, du cas 2 vers l'état *détruit*. Chacune de ces *output gate* aura sa propre fonction de sortie ($f : M_G \rightarrow M_G$, avec $(G \subseteq P)$) qui déterminera l'évolution du marquage (passage à 1 du marquage de la place de sortie concernée et mise à 0 du marquage de la place en amont de l'activité). La structure du réseau correspondant à cet exemple, qui définit la modélisation des états *détérioré* et *détruit*, est présentée à la figure 4.3.
Pour continuer dans la définition du modèle SAN de l'atome conceptuel, nous nous intéressons aux activités liées à la régénération. Relativement aux mécanismes présentés à la section 4.1.2, les relations $\mathscr{R}_6$ et $\mathscr{R}_7$ caractérisant l'échange de constituant imposent de prendre en compte les stocks. Ces stocks peuvent être issus d'un lot de bord du système de soutien ou encore d'une possibilité d'interchangeabilité. Pour ce faire, nous introduisons dans le modèle de constituants des places représentatives du stock. Le marquage de cette place interviendra dans la fonction d'activation de l'*input gate*, liée à l'activité d'échange. De la même manière, les activités de réparation d'un constituant en panne ou détérioré, sont limitées par le nombre de réparations supportées par le constituant (cf. relation $\mathscr{R}_8$). Des places supplémentaires sont donc également introduites en amont des activités de réparation. Enfin, l'activité de reconfiguration qui conduit à l'état "en_reconfiguration"

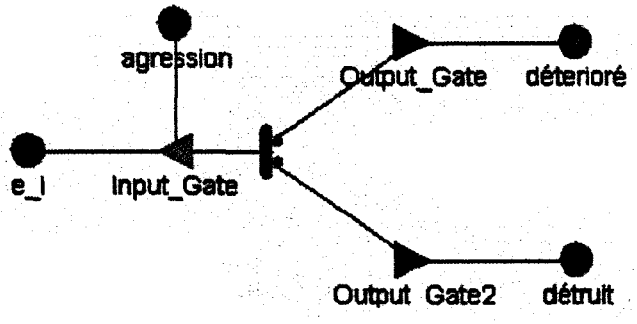

FIG. 4.3 – Structure du modèle SAN pour la représentation des agressions et des dommages.

lie nécessairement deux constituants. La relation $\mathscr{R}_{10}$, qui intervient dans la construction du modèle SAN du constituant au niveau de l'activité reconfiguration, impose de considérer l'état du constituant atteint dans la définition de l'activité de reconfiguration pour le constituant qui va effectuer la reconfiguration. Ainsi, on introduit au niveau du modèle les places représentatives des états qui nécessitent la reconfiguration dans le modèle. Par exemple, dans le cas d'un constituant qui entre en reconfiguration si un autre constituant passe dans l'état "détruit" ou "panne", les places "panne" et "détruit" du constituant à l'origine de la reconfiguration seront reportées dans le modèle. Le marquage de ces places sera considéré dans l'*input gate* au niveau de la fonction d'activation de la porte en amont de l'activité "reconfiguration". Nous pouvons maintenant présenter un modèle SAN complet d'un constituant qui intègre la modélisation présentée à la figure 4.3 ainsi que les différentes places supplémentaires telles que nous venons de le définir. Ce modèle est présenté à la figure 4.4. Chaque *input gate* intègre une fonction d'activation qui va dépendre d'une équation sur le marquage d'un sous-ensemble de places et les *output gates* permettent de définir les évolutions de marquage après la réalisation des différentes activités.

Nous avons illustré dans cette partie l'utilisation du formalisme des SANs comme support de l'atome conceptuel de modélisation du comportement des constituants. L'exploitation des mécanismes de construction définis à la section 4.1 a également été détaillée. Ces mécanismes nous ont conduit dans un premier temps à introduire des places supplémentaires de manière à considérer l'ensemble des éléments prescrits par ces mécanismes et, dans un deuxième temps, leur utilisation dans la définition du comportement du constituant à travers l'écriture de fonction d'activation des *input gates* a été présentée. Aussi, l'exploitation de l'ensemble des mécanismes défini nous permet la construction d'un modèle dynamique particulier, représentatif du comportement des constituants dans le respect de la description du système faite dans le modèle structurel. La construction d'un modèle dynamique complet implique donc de construire autant de modèles atomiques de constituants que de constituants dans le système complet. On aura donc

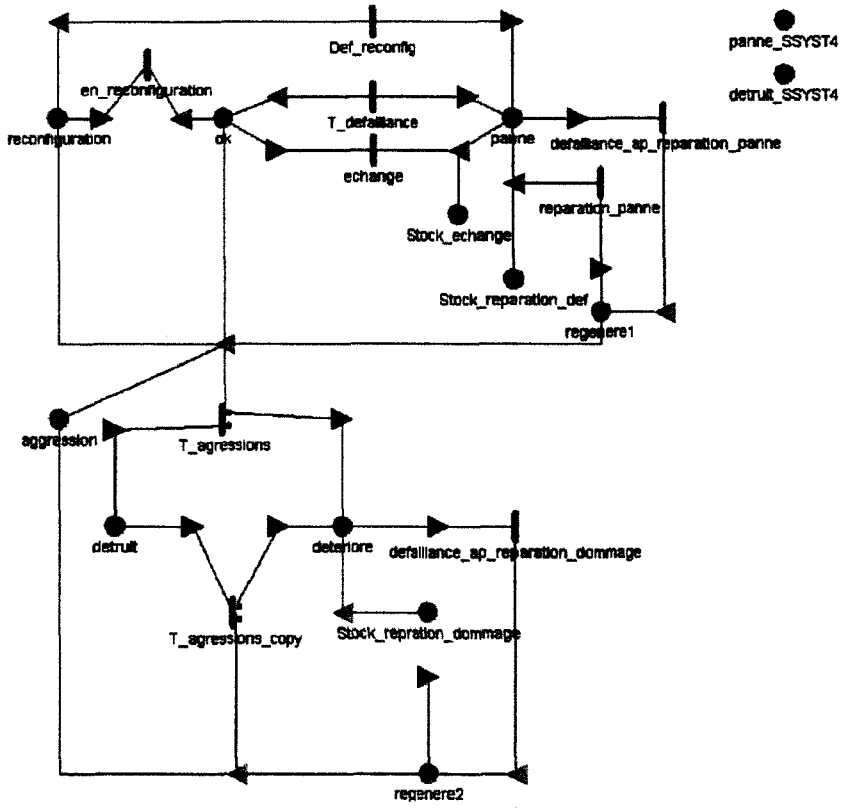

FIG. 4.4 – Modèle SAN d'un constituant.

$n_{modèle\ atomique\_constituant}) = Card(C)$, où $C = \{Constituant\}$. La partie suivante est consacrée au modèle atomique SAN représentatif du comportement des fonctions.

Modèle SAN de l'atome de modélisation des fonctions

Chaque fonction est représentée par quatre états {nominal, dégradé, secours, panne}. Le passage d'un état vers un autre est déterminé par l'état de chacun des constituants supports de la fonction relativement à la relation $\mathscr{R}_{12}$ définie à la section 4.1.3. La figure 4.5 rappelle le modèle atomique conceptuel d'une fonction. Pour chacune des fonctions les changements d'états suivants seront considérés :

- {nominal} → {dégradé}
- {nominal, dégradé} → {secours}
- {nominal, dégradé, secours} → {panne}
- {panne} → {secours}
- {secours, panne} → {dégradé}

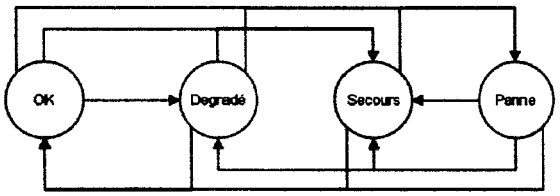

FIG. 4.5 – Modèle atomique conceptuel d'une fonction

– {dégradé, secours, panne} → {nominal}

Cette écriture permet de réduire le nombre des relations à définir. Conformément au formalisme des SANs, les relations de type $\mathscr{R}_{12}$ qui déterminent le passage d'un état vers un autre seront introduites au niveau des fonctions d'activation des *input gates* déterminant ainsi les conditions de validation des activités représentant les changement d'états. Aussi, comme l'activité de reconfiguration dépend du marquage des places représentatives de certains états d'autres constituants, les règles d'agrégation seront écrites à partir du marquage des places représentatives des états des constituants. Pour ce faire, les places correspondant aux états dans le modèle atomique des constituants seront rapportées dans le modèle de la fonction. A chaque activité du modèle atomique d'une fonction sera associée une *input gate* dont la fonction d'activation est une équation combinatoire du marquage des places relatives aux constituants. Un exemple de modèle SAN d'une fonction est donné à la figure 4.6[3]. Dans cet exemple la fonction considérée est supportée par deux constituants notés : SSYST_1 et SSYST_2. A titre d'exemple, nous donnons la fonction d'activation de l'*input gate* liée à l'activité menant dans l'état "panne" (*input gate* notée "OK_D_S_vers_panne" dans la figure 4.6) :

$$\Big((\mathscr{M}_{f\_secours} = 1 \vee \mathscr{M}_{f\_degrade} = 1 \vee \mathscr{M}_{f\_ok} = 1) \wedge (\mathscr{M}_{panne\_SSYST\_1} = 1 \vee \mathscr{M}_{detruit\_SSYST\_1} = 1 \vee \mathscr{M}_{panne\_SSYST\_2} = 1 \vee \mathscr{M}_{detruit\_SSYST\_2} = 1)\Big)$$

Cette fonction d'activation détermine donc les conditions de passage dans l'état "panne" pour la fonction. Si la fonction se trouve dans un état "ok" ou "dégradé" ou "secours" et que l'un de ses 2 constituants supports (SSYST_1 ou SSYST_2) passe dans l'état "détruit" ou "panne", la fonction passe alors dans l'état panne. Au niveau des fonctions, les activités considérées sont toutes des activités instantanées, les instants de passage étant régis par l'évolution des constituants. Comme pour les constituants, la construction d'un modèle dynamique complet comprenant plusieurs fonctions nécessitera autant de modèles atomiques de fonctions que de fonctions dans le système considéré, soit : $m_{modèle\ atomique\_fonction} = Card(F)$, où $F = \{fonctions\}$.

Pour permettre l'évaluation, le modèle dynamique doit être supporté par un outil qui intègre à la fois le formalisme des SANs dans leur partie structurelle (construction des

[3]Dans ce modèle, seuls les input gates ne sont étiquetées dans la mesure où ce sont elles qui portent les équations d'agrégation.

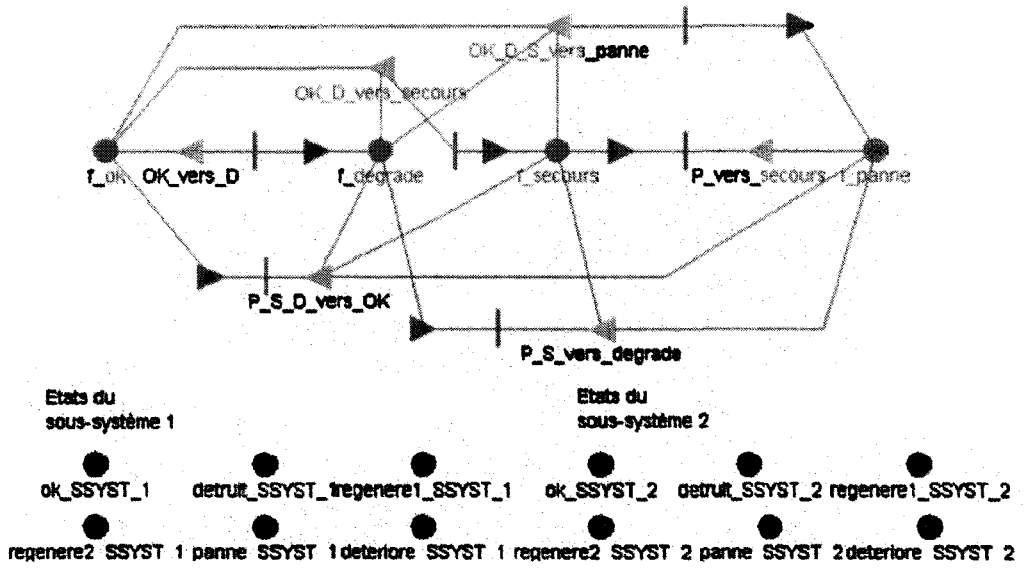

FIG. 4.6 – Modèle atomique SAN d'une fonction supportée par les constituants SSYST_1 et SSYST_2

réseaux) mais aussi la définition des variables de récompense et enfin des possibilités de simulations.

4.2.3 Outil support des modèles SAN pour la construction et l'évaluation des modèles

Depuis leur introduction, les SAN ont servi de base au développement de trois outils de modélisation : META*SAN* (W.H. Sanders et J.F. Meyer 1986), ULTRA*SAN* (W.H. Sanders et al. 1995) et, le plus récent, Möbius (D. Daly et al. 2000, G. Clark et al. 2001). L'ensemble des modèles atomiques supports de l'évaluation de la disponibilité opérationnelle des architectures de systèmes de système ont donc été réalisés à l'aide de l'outil Möbius[4]. En effet, l'outil Möbius intègre tous les aspects nécessaires à :

1. la construction des modèles atomiques,
2. la composition hiérarchique des modèles atomiques,
3. la définition des variables de performance,
4. la simulation du modèle pour l'évaluation des variables de performance.

L'outil Möbius fournit par ailleurs un environnement ouvert avec la possibilité de construire l'ensemble des fonctions relatives aux *input* et *output gates* ainsi que l'ensemble des pa-

[4]Informations disponibles sur http ://www.mobius.uiuc.edu/index.html

ramètres des activités en fonction du marquage des différentes places du réseau dans le langage C++.

Construction des modèles Atomiques

La construction des modèles atomiques est basée sur une interface graphique qui permet de *dessiner* directement le réseau représentatif du système. Les différents éléments du modèle sont ensuite paramétrés par l'intermédiaire de propriétés (e.g. marquage initial pour les places, type de distribution/paramètres/probabilités affectés aux cas pour les activités,...). A titre d'exemple, la définition de l'activité liée aux défaillances est présentée à la figure 4.7 : le délai correspondant à la réalisation de l'activité correspond au temps de bon fonctionnement du constituant évalué à partir d'un tirage aléatoire et du taux de défaillance du constituant qui est ici un paramètre global[5]. L'outil Möbius offre donc une très grande flexibilité dans la modélisation avec la possibilité notamment de définir des expressions complexes dépendant à la fois du marquage et d'autres paramètres au niveau des délais associés aux activités.

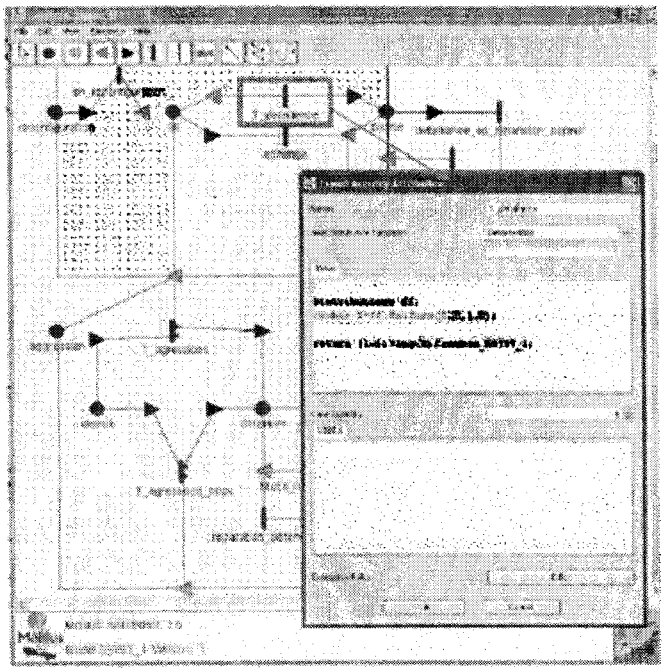

FIG. 4.7 – Exemple de paramétrage de l'activité "défaillance" dans le modèle d'un constituant.

[5]L'utilisation de paramètres globaux permet d'en modifier les valeurs dans le cas de la réalisation d'un plan d'expériences.

De la même manière, les probabilités liées aux différents cas de l'activité "agressions", représentatives des probabilités d'être détruit ou détérioré sont ainsi définies. Dans l'exemple considéré ici pour illustrer l'utilisation de Möbius, quatre modèles atomiques ont été réalisés (2 constituants, 1 fonction et un modèle d'agression). Chaque modèle atomique est ainsi construit et paramétré avant de donner l'architecture globale du modèle définie par le modèle composé.

Construction du modèle composé

Une fois l'ensemble des modèles atomiques réalisé, il est nécessaire de donner l'architecture globale de l'application construite. Pour ce faire, Möbius offre des possibilités de modélisation hiérarchique et modulaire basées sur le formalisme *Replicate/Join*, (A. Stillman 1999). Le formalisme *Replicate* permet notamment de réduire considérablement l'espace d'états quand les systèmes considérés présentent des symétries. Relativement à notre application, le formalisme *Join* nous permet de partager des variables d'états entre les modèles. Ainsi, le modèle composé définit une structure arborescente représentative des relations de contribution des constituants aux fonctions. Nous définissons donc un modèle *Join* par fonction lié aux modèles atomiques de la fonction, des constituants supports et du modèle d'agression. Ce modèle est ensuite configuré de manière à ce que les variables d'états associées aux places représentatives des états des constituants dans le modèle de la fonction (cf. figure 4.6) soient partagées avec les variables d'états associées aux places des modèles atomiques des constituants. Ainsi, à chaque instant de la simulation, le marquage des places représentatives des états des constituants du modèle de la fonction est exactement le même que le marquage des places dans le modèle atomique des constituants, qui lui évolue en fonction des différentes distributions de probabilités et des différents tirages aléatoires. Ce formalisme nous permet donc de rendre effectif le principe d'agrégation utilisé pour déterminer l'état d'une fonction en fonction de l'état de ses constituants supports. Ce mécanisme est illustré à la figure 4.8 avec le partage de la place "OK" entre le modèle du constituant "SSYST_1" et le modèle de la fonction "OBS_1". La structure arborescente associée au partage de variable d'état permet notamment de partager des places à différents niveaux et entre tous les modèles offrant ainsi une grande flexibilité dans la modélisation, notamment pour la prise en compte des relations d'interactions entre les constituants et entre les fonctions .

Définition des variables de performance

Möbius permet de définir un modèle de récompense pour l'évaluation des variables de performance. Une variable de performance est définie en associant soit un taux de récompense en fonction du marquage d'un modèle, soit une récompense en fonction de la réalisation d'une activité. Une variable de récompense peut donc être une expression complexe représentative d'une configuration particulière du système représentée par un marquage particulier de chacun des modèles atomiques (cf. section 4.2.2). Pour l'évaluation de performance telle que la disponibilité, les variables de performances vont nous permettre d'évaluer les temps de séjour dans des états particuliers représentatifs d'un

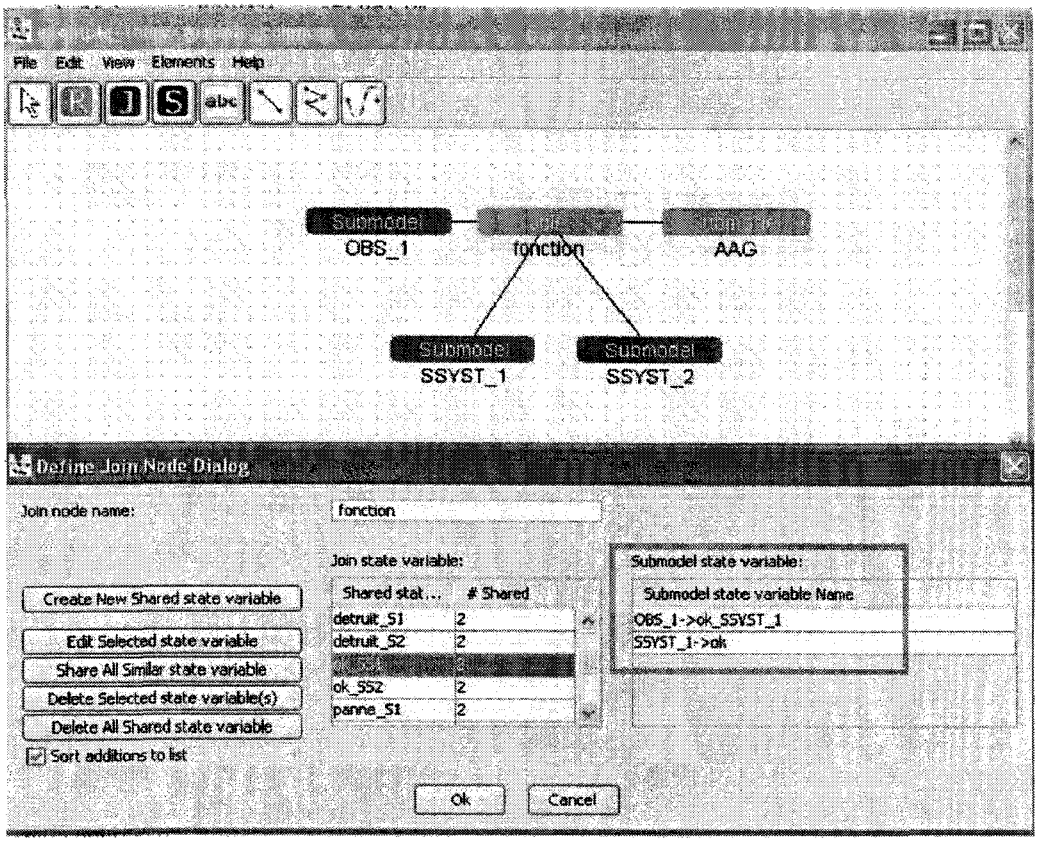

FIG. 4.8 – Modèle composé et partage de variables d'états

état fonctionnel du système. On peut, par exemple, s'intéresser au temps de séjour dans les états fonctionnels d'un constituant, la variable de performance correspondante est présentée dans la table 4.2. La variable de performance est basée sur l'accumulation de la récompense quand le constituant se trouve dans un des trois états {ok, regeneré1, régénéré2}. Aussi, la disponibilité du constituant peut être estimée en évaluant la variable de performance sur un intervalle de temps donné ; ici [0.0 - 100]. L'intervalle de confiance permet de spécifier la précision des résultats attendus et constitue un critère d'arrêt de la simulation.

Simulation des modèles

Pour l'analyse des modèles, nous utilisons les simulations de Monte Carlo qui permettent d'avoir des estimations des grandeurs de sûreté de fonctionnement à partir de modèles décrivant des systèmes ne respectant pas l'hypothèse de Markov. Möbius est un outil particulièrement adapté aux simulations de Monte carlo sur la base d'une simula-

TAB. 4.2 – Exemple de variable de performance

Etat_fonctionnel_SSYST_1		
Fonction de récompense		
if (SSYST_1->ok->Mark()==1 || SSYST_1->regenere1->Mark()==1 ||		
SSYST_1->regenere2->Mark()==1)		
{		
return 1;		
}		
Statistique de Simulation	Type	Intervalle de temps
	Paramètres	Temps début 0.0
		Temps fin 100
	Précision	Niveau de confiance 0.95
		Intervalle de confiance 0.1

tion à événements discrets, (A. Williamson 1998). En effet, Möbius propose notamment un choix entre deux générateurs aléatoires et offre la possibilité de donner une séquence d'initiation du générateur, ce qui permet de jouer les mêmes histoires pour comparer des configurations différentes ou de changer l'initialisation et avoir ainsi des histoires différentes. L'ordonnanceur du simulateur évalue les délais associés à toutes les activités valides pour le marquage atteint et la prochaine activité dans le temps relativement au temps courant du simulateur sera réalisée. La simulation permet donc d'estimer l'ensemble des variables de performance sur la base des processus stochastiques définis au niveau des modèles atomiques des constituants. Pour prendre en compte l'ensemble des paramètres globaux des différents modèles atomiques, les simulations doivent être associées à un fichier d'*étude* qui rassemble l'ensemble des paramètres globaux des modèles à définir, on définit alors une *Set study*. L'outil propose deux critères d'arrêt des simulations :

- la convergence des variables de performances est atteinte relativement à l'intervalle de confiance défini dans le modèle de récompense,
- le nombre maximum de simulations défini dans la définition des simulations est atteint.

L'ensemble des résultats est ensuite formaté dans un fichier *.txt* et un fichier *.csv* pour être exploités. La figure 4.9 donne un aperçu d'une simulation.

4.2.4 Conclusion

Parmi les principaux formalismes susceptibles de supporter le modèle dynamique dans le respect des mécanismes de construction introduits à la section 4.1, nous avons montré comment les Stochastic Activity Networks constituent un support privilégié à

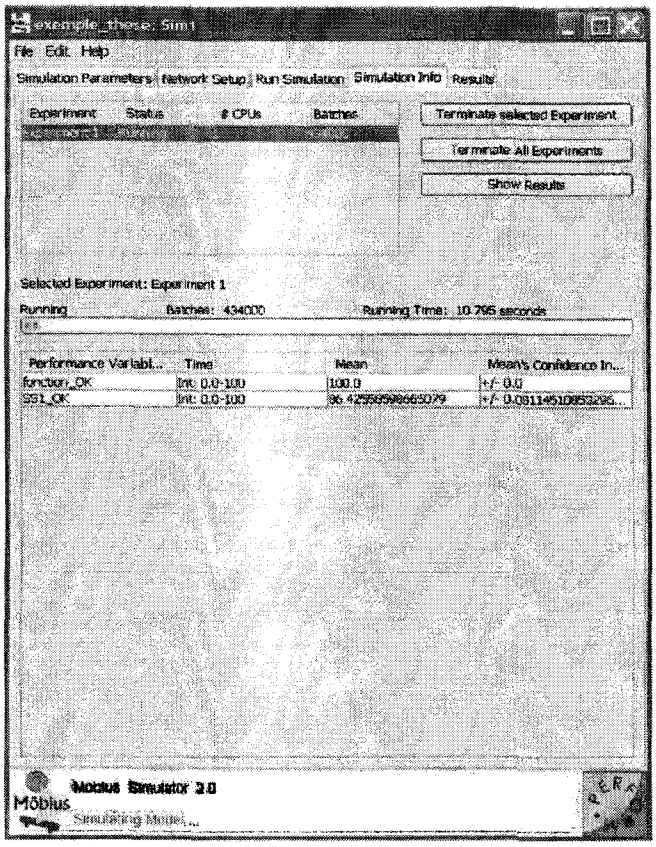

FIG. 4.9 – Copie d'écran de la fenêtre pendant une simulation.

la modélisation. Chaque aspect dans la modélisation nécessaire pour rendre compte du comportement de systèmes en présence de défaillances, de dommages et de régénération pour l'évaluation de la disponibilité opérationnelle peut être considéré au sein de la modélisation SANs. Ensuite, nous avons illustré l'ensemble de principes de modélisation relatifs aux SANs à travers l'exploitation de l'outil de modélisation Möbius qui permet à la fois de construire et d'évaluer les modèles. Cet outil est particulièrement adapté à la démarche de modélisation hiérarchique et modulaire définie dans le contexte plus général d'ingénierie de régénération proposé dans nos travaux. L'outil supporte donc la construction des modèles dans le respect des mécanismes de construction et fournit un support aux simulations de Monte Carlo pour l'évaluation des variables de performance. La flexibilité de modélisation offerte par les SANs au sein de l'outil Möbius permet de construire un ensemble de variables de performance plus ou moins complexes qui, associées à un traitement statistique, permettent de représenter les grandeurs significatives de sûreté de fonctionnement.

4.3 Conclusion

Dans ce chapitre, nous avons abordé la deuxième partie de notre contribution consacrée au modèle dynamique support des évaluations des performances de sûreté de fonctionnement et, notamment, de la disponibilité opérationnelle. Sur la base de la description du système réalisée au sein du modèle structurel décrit dans le chapitre III, nous avons donc tout d'abord défini un ensemble de mécanismes de construction génériques permettant de contraindre la construction des atomes de modélisation des constituants et des fonctions. Ces mécanismes sont relativement généraux mais permettent cependant de guider l'utilisateur dans sa modélisation sans contraindre le choix d'un technique particulière de modélisation des atomes. Aussi, sur la base des principales techniques de modélisation de type état-transition utilisées en sûreté de fonctionnement, nous proposons ensuite l'utilisation des Stochastic Activity Networks comme support aux modèles atomiques à la base du modèle dynamique. En effet, les SANs qui correspondent à une extension des réseaux de Petri stochastiques offrent à la fois la puissance de représentation des réseaux de Petri, la flexibilité des stochastic reward nets et constituent enfin un très bon support aux simulations de Monte Carlo qui permettent de traiter des grands systèmes non markoviens. L'intérêt et la faisabilité de l'utilisation des SANs dans le respect des mécanismes de construction ont ensuite été montrés à travers l'exploitation de l'outil Möbius, support à la modélisation SAN. Cet outil permet de prendre en compte l'ensemble des aspects nécessaires à la modélisation et offre la possibilité de simuler les modèles pour l'estimation des performances des systèmes.
Le cinquième chapitre de ce mémoire est donc consacré au développement d'un cas d'application représentatif de l'ensemble de la démarche proposée dans nos travaux afin d'en montrer, à une échelle réaliste, l'intérêt et la faisabilité.

Chapitre 5

Evaluation de la disponibilité opérationnelle d'une architecture de système de systèmes

Ce chapitre est consacré à la mise en oeuvre de la démarche de modélisation proposée pour l'ingénierie de régénération. Une architecture typique de SdS, sur laquelle la DGA travaille pour la mise en oeuvre de principes de régénération, sera tout d'abord présentée. Sur la base de cette architecture, nous définirons ensuite une architecture réduite mais représentative de la problématique pour la mise en oeuvre de la démarche et la construction des modèles. Ceci nous permet ainsi de démontrer la faisabilité de la démarche en y apportant des éléments de validation. Nous montrerons comment les modèles construits peuvent être utilisés pour évaluer tant des solutions de conception de plates-formes que des solutions de conception d'architectures de SdS. L'ensemble des résultats de simulation obtenu sera également discuté.

5.1 Introduction

Dans les chapitres III et IV, nous avons proposé une méthodologie de modélisation pour l'ingénierie de régénération adaptée à l'évaluation de la disponibilité opérationnelle des systèmes d'armes en présence de défaillances, de dommages et de régénération. Pour valider la démarche, il est nécessaire de l'appliquer sur une architecture de système représentative de la problématique intégrant des constituants, des fonctions ainsi qu'un scénario opérationnel.
En ce sens, le chapitre V décrit la mise en oeuvre de la méthodologie développée sur une architecture définie en partenariat avec la DGA et NEXTER systems. Cette architecture s'inspire des architectures globales de SdS et correspond, compte tenu des délais impartis par la thèse, à une vision réduite d'une telle architecture. Ce chapitre s'attache donc dans un premier temps à présenter une architecture de SdS concrète. L'architecture retenue pour la validation de la démarche ainsi qu'un exemple de scénario opérationnel associé sont ensuite présentés. Les différentes étapes de la méthodologie seront ensuite abordées relativement à l'architecture retenue. Différentes solutions de régénération sont envisagées ainsi que différentes architectures afin de montrer les possibilités offertes par la démarche proposée pour l'évaluation de la disponibilité en fonction des possibilités de régénération.

5.2 Le SGTIA : des architectures au coeur de la BOA

La méthodologie de modélisation proposée a été développée de manière à pouvoir considérer des architectures de SdS définies relativement au nouveau concept de BOA. Ces architectures correspondent aux architectures possibles pour un Sous-Groupement Tactique Inter-Armes (SGTIA). En effet, tel qu'elle est définie, la BOA met en oeuvre un système de Cohérence de Combat de Contact (SC^3) basé sur des architectures particulières de SGTIA. Aussi, l'architecture du SC^3 doit être modulaire et adaptative pour permettre la constitution de SGTIA de tailles variables et de capacités différentes en mobilité tactique ou stratégique, observation, agression et protection, (N. Rosain et X. Le Vern 2004). Dans notre objectif d'évaluation de la disponibilité opérationnelle de telles architectures en présence de défaillances, de dommages et de régénération, nous verrons comment la méthodologie proposée permet d'obtenir les modèles supports aux simulations pour l'évaluation des performances de disponibilité.

5.2.1 Présentation générale d'un SGTIA

Les industriels impliqués dans la définition de la BOA travaillent actuellement à la définition d'architecture de SGTIA, (H. Laporte 2004). Aussi, il existe différentes façons de décrire un SGTIA, les descriptions fournies dans la suite correspondent à une synthèse des travaux menés par NEXTER (anciennement Giat) (N. Rosain et X. Le Vern 2004), EADS et MBDA, (H. Laporte 2004).

Un SGTIA est défini relativement à la mission qui lui est assignée ; aussi, les architectures sont décrites d'abord suivant un point de vue fonctionnel, puis on définit une architecture concrète dans laquelle on décrit les plates-formes associées au SGTIA répondant à l'architecture fonctionnelle.

5.2.2 Description des architectures fonctionnelles

Pour décrire une architecture fonctionnelle, il suffit de décrire chaque plate-forme de chaque élément de manoeuvre. La répartition des éléments de manoeuvre au sein du SGTIA et la répartition des plates-formes au sein des éléments de manoeuvre découlent des architectures opérationnelles définies par la mission.

Pour décrire une plate-forme, on précise tout d'abord sa fonction principale et ensuite sa ou ses fonctions secondaires. Les fonctions du socle commun sont, par définition, toutes réalisées par toutes les plates-formes. Elles ne sont donc pas rappelées (elles seront néanmoins prises en compte lors de l'implantation).

Les **fonctions du socle commun**, à chaque plate-forme, sont :

- Observation « de base »,
- Protection individuelle,
- Mobilité,
- Communication,
- Système d'information,
- Fusion « locale ».

Les **fonctions principales** : une plate-forme assure une fonction principale, c'est la fonction pour laquelle elle a été conçue.

- Commandement,
- Tir « direct »,
- Tir « au delà de la vue directe »,
- Observation,
- Génie,
- Logistique,
- Observation,
- Drônes et robots,
- Observation d'artillerie.

Les **fonctions secondaires** : en plus de sa fonction principale, une plate-forme peut réaliser une ou plusieurs fonctions secondaires (différentes de la fonction principale). Les moyens nécessaires à la réalisation de ces fonctions sont ajoutés à la plate-forme.

- Observation « évoluée »
- Protection collaborative au niveau EI[1]
- Commandement
- Tir direct
- Tir au delà de la vue directe
- Drone

[1] EI :Element Intermédiaire

- Robot
- Fusion - consolidation
- Gestion des capteurs et effecteurs
- Support SIC[2]

5.2.3 Description des architectures concrètes

La description d'une architecture concrète consiste, à partir de l'architecture fonctionnelle, à associer une plate-forme concrète à chaque pion fonctionnel. Une plate-forme concrète est décrite en indiquant sa famille (XL[3], EBRC[4], VBCI[5],...) et l'ensemble des équipements qui la composent (moyens d'observation, de feu, système d'information et de communication,...). Selon qu'elle correspond à tel ou tel pion fonctionnel, une plate-forme peut voir sa dotation varier. On voit ainsi apparaître plusieurs types de plates-formes par famille.

Les familles de plate-formes sur lesquelles les fonctions présentées au paragraphe précédent sont implantées, correspondent aux plate-formes suivantes :

- Char Leclerc (XL),
- EBRC,
- VBCI,
- VAB[6],
- VOA[7],
- 2R2M : véhicule transportant le mortier de 120 mm,
- Camion CAESAR.

Ensuite, pour chaque pion fonctionnel, on détermine un ou plusieurs types de plates-formes adéquats et on définit la dotation en équipements pour identifier la plate-forme retenue. La table 5.1 donne par exemple une architecture concrète à *dominante blindé léger*.

5.2.4 Description des plates-formes

Pour constituer l'architecture finale du SGTIA, on décrit les plates-formes en termes de fonctions et d'équipements. Pour chaque famille, les plates-formes sont dotées d'équipements particuliers de manière à supporter les fonctions opérationnelles attendues. La table 5.2 décrit à titre d'exemple une plate-forme de la famille EBRC dont la fonction principale serait Tir « au delà de la vue directe » (cf. section 5.2.2).

Le SGTIA qui constitue le système de contact est donc vu comme un SdS défini en terme de capacités opérationnelles globales (liées à sa mission), ses performances globales étant déclinées et allouées sur les différentes plates-formes (systèmes d'armes) au

[2]SIC :Système d'Information et de Communication

[3]XL : Char Lelclerc

[4]EBRC : Engin Blindé à Roues de Contact

[5]VBCI : Véhicule Blindé de Combat de l'Infanterie

[6]VAB :Véhicule de l'Avant Blindé

[7]VOA :Véhicule d'Observation d'Artillerie

TAB. 5.1 – Exemple d'architecture concrète

Dominante « blindé léger »	
EM de commandement	1 EBRC CDT SGTIA
	1 VAB SAN
	1 VOA
	1 P4
	1 moto
EM de combat direct (× 2)	1 EBRC canon 105 + CDT EM
	3 EBRC canon 105
EM de combat direct (× 1)	1 VBCI version VCI CDT EM
	1 VBCI version VCI ACCP tir direct
	2 VBCI version VCI
EM de combat indirect (× 1)	1 EBRC canon 105 MIM SAL + CDT EM
	2 EBRC canon 105 MIM SAL
EM de renseignement	1 EBRC Rens
	2 EBRC drone / robot

sein desquelles les fonctions du système de contact sont réparties. Aussi, l'ensemble des descriptions présentées ci-avant constitue donc la base de la définition d'une architecture de SGTIA. Toutes ces données relatives aux aspects organico-fonctionnels de l'architecture doivent être complétées par un scénario opérationnel des systèmes afin de disposer de l'ensemble des éléments pour la construction du modèle structurel correspondant. Dans la suite, nous présentons le scénario opérationnel retenu pour servir d'exemple à l'application de la méthodologie proposée dans nos travaux.

5.3 Architecture retenue

Le scénario décrit dans cette section a été fourni par la société NEXTER en accord avec la DGA, pour servir de base à la construction d'un scénario de validation de la méthodologie. Le scénario présenté met en action une section de VBCI, engagée dans une mission de reconnaissance d'un point particulier, face à une menace missile, tiré à partir d'un blindé lance-missiles antichar. L'ensemble décrit dans ce scénario correspond donc à un sous ensemble d'une architecture complète de SGTIA dans le sens où la section VBCI est assimilée à un élément de manoeuvre associé à une fonction de renseignement tel que celui défini dans la table 5.1 où les VBCI remplaceraient les EBRC. Cet exemple d'architecture réduite mais non réductrice nous permet d'illustrer les principaux éléments de la méthodologie et d'apporter des éléments de validation et correspond une extension des travaux présentés dans (M. Monnin, O. Senechal et B. Iung 2007b, M. Monnin et al.

TAB. 5.2 – Exemple de description d'une plate-forme

Plate-forme	**EBRC Missile - canon 40 mm**
FEU	1 poste de tir missile + 6 missiles NLOS HdlB (portée 6/8 km)
	1 canon de 40 mm CTA
	Mitrailleuse
PROTECTION	S/E DIC
	S/E Soft-Kill complet
	S/E Hard-Kill "protection active" léger
	S/E Alerteurs étendus (uniquement pour le Cdt d'EM)
	Kit S/E Armes Non Létales (en maîtrise de la violence en ZU)
OBSERVATION	Viseur chef de bord EBRC (CCD, CT, télémètre/désignateur)
	Viseur tireur EBRC (CCD, CT, télémètre) SI/Fusion
SI[8]/Fusion	Equipement standard
COMMUNICATION	Poste radio BOA (voix / données)
	Liaison de données avec le robot
DRONE/ROBOTS	Minidrone d'observation
EQUIPAGE	personnes : 1 chef de bord, 1 pilote, 1 tireur, 1 opérateur drone

2008).

Il est à noter que pour des raisons de confidentialité, l'ensemble des éléments (structure, données, résultats) présentés dans la suite n'a de valeur qu'en terme d'illustration de la méthodologie. Les grandeurs utilisées ne sont pas des données réelles et ont été introduites uniquement dans le but de pouvoir mettre en oeuvre la démarche pour en montrer sa faisabilité.

5.3.1 Description d'un scénario opérationnel

Le scénario opérationnel associé à l'élément de manoeuvre de renseignement supporté par 4 VBCI est illustré par le schéma de la figure 5.1. La description *textuelle* du scénario fourni par NEXTER est la suivante : *Lors de l'infiltration, la section progresse rapidement en colonne. A l'approche de la zone, les VBCI se séparent (cf. figure 5.1) : 2 restent face au pont en observation et appuient la progression des 2 autres qui cherchent à s'infiltrer au plus près du point à reconnaître. En traversant une zone découverte pour rejoindre un poste, le second est pris à partie par un missile antichar de type AT11. L'alerte DDM du VBCI active ses fumigènes et ce dernier accélère son mouvement pour rejoindre une position à l'abri. Son déplacement s'effectue de manière erratique pour rendre plus difficile la visée du tireur missile. Compte tenu de la distance de tir (<1000m), ses chances de survie sont très réduites. Les informations concernant la menace sont disponibles (gise-*

ment) et sont transmises automatiquement à l'un des deux VBCI en appui (informations posthumes). Ces informations sont traitées et affichées sur la cartographie SIT du VBCI destinataire; avec la dernière position du VBCI et le gisement de la menace, le VBCI peut apprécier la position ennemie possible. Le chef d'engin étudie rapidement les positions possibles de l'ennemi en suivant le tracé du segment sur sa cartographie; ce segment est orienté selon le gisement reçu avec comme origine la dernière position du VBCI. L'un des VBCI en appui manoeuvre pour prendre une position de tir et engage par le feu la position supposée de l'ennemi. Le poste de tir ennemi est fixé, voire détruit. Le peloton a perdu (sans doute) un engin mais la mission est remplie par l'obtention des renseignements : le point est défendu par un ennemi débarqué et localisé. En ce sens, notre méthodologie par le biais de l'évaluation de la disponibilité opérationnelle va permettre de rendre compte de la probabilité de réussite de la mission. En effet, la DGA a défini un critère de réussite de mission tel que : la mission est réussie si le système est disponible pendant au moins 95% de la durée de la mission. Aussi, compte tenu de l'architecture définie pour accomplir la mission de renseignement, la mission sera considérée comme réussie si les deux fonctions d'observation et au moins une des fonctions FEU sont disponibles pendant 95% de la durée de la mission. Cette description nous permettra de développer les variables de performance pour l'évaluation.

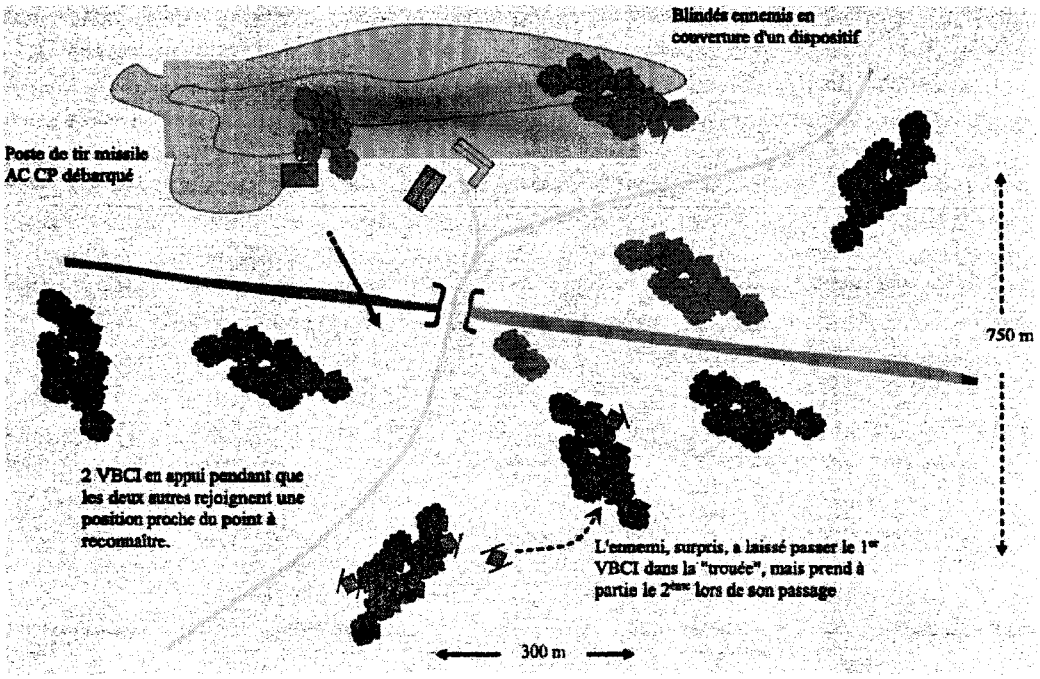

FIG. 5.1 – Exemple d'illustration d'un scénario opérationnel

Cette description de la mission est ensuite complétée avec des données précises sur la menace (table 5.4) et sur la situation initiale des différentes plates-formes. Toutes ces

données (description de la mission, données sur la menace et situation initiale) permettent aux experts de déterminer notamment les données de vulnérabilité relatives à ce scénario opérationnel particulier, nécessaires à la simulation.

TAB. 5.3 – Caractéristiques techniques de la menace

Plate-forme de tir	Poste portable (4.8kg)
Nom	AT-11 Metis M
Type	Anti-Char courte portée
Guidage	Filoguidé $2^{ème}$ génération
Portée minimale	50m
Portée maximale	1000m
Vitesse départ V_0	200m/s
Vitesse maximale V_{max}	300m/s (environ)
Temps de vol	6s à 1000m ; 5s à 750m
Temps engagement second véhicule	> 20s après fin du guidage premier missile

Pour notre application, nous supposons que cette mission a une durée de 24 heures, et que la probabilité d'occurrence de la menace est de 0.8, pour la mission considérée.

5.3.2 Description de l'architecture organico-fonctionnelle

La description du scénario opérationnel et de l'architecture proposée pour supporter les capacités opérationnelles attendues nous permettent tout d'abord de définir une architecture organico-fonctionnelle, comme première étape à la formalisation des connaissances pour la modélisation. L'architecture proposée est présentée à la figure 5.2. Elle compte donc 4 plates-formes : 2 plates-formes d'observation correspondant aux 2 VBCI qui avancent vers le point à reconnaître et 2 plates-formes de feu correspondant aux 2 VBCI en appui. La fonction de renseignement est donc globalement supportée par une fonction d'observation (qui va dépendre des 2 fonctions d'observation) et une fonction feu (qui dépend des deux fonctions feu). Chaque plate-forme sera donc représentée par sa fonction principale et les constituants qui la supportent. On suppose dans cet exemple que chaque fonction est supportée par deux constituants notés SSYST_1 à SSYST_8 (pour sous-système). Nous avons maintenant les premiers éléments descriptifs du système dans son contexte opérationnel (durée de la mission, probabilité d'occurrence de la menace, architecture retenue pour effectuer la mission), il reste donc à préciser les possibilités de régénération envisageables pour l'architecture considérée. Trois scénarios ont été envisagés afin de rendre compte des possibilités d'évaluation de la méthodologie.

5.3.3 Description des scénarios de régénération

La méthodologie de modélisation proposée nous permet d'évaluer la disponibilité opérationnelle d'architectures de SdS militaires en présence de défaillances, de dommages et

TAB. 5.4 – situation initiale

	VBCI 1	VBCI 2	VBCI 3	VBCI 4
Position du châssis / Menace	De flanc	De $\frac{3}{4}$ avant	De face	De face
Position de la tourelle	De $\frac{3}{4}$ avant	De $\frac{3}{4}$ avant	De face	De face
Attitude au moment de l'agression ennemie	En mouvement rapide	En mouvement lent	A l'arrêt	A l'arrêt
Masque avec le poste de tir	Oui	Non	Oui	Oui
Masques proches	Aucun	Oui	Oui	Oui
Intervisibilité entre amis	Non avec aucun autre VBCI	Non	Non	Non
Intervisibilité potentielle avec la menace	Oui	Non	Non	Non
Action en cours	Déplacement	Déplacement	Observation et prêt à tirer	Observation
Météo	Temps clair bonne visibilité			

de régénération. Afin d'illustrer tous les aspects relatifs aux dommages et à la régénération, nous présentons les trois scénarios envisagés.

Scénario 1

Le premier scénario a pour objectif de montrer l'impact des agressions sur la disponibilité opérationnelle. La mission sera donc considérée une première fois en l'absence de menace, les seuls facteurs d'indisponibilité seront ceux liés aux défaillances intrinsèques et aucune régénération n'est possible.

Scénario 2

Le deuxième scénario tend à montrer l'impact de la régénération sur la disponibilité opérationnelle. L'action de régénération considérée dans ce scénario (figure 5.3) est la même que dans (M. Monnin, B. Iung et O. Sénéchal 2007a) : on suppose que le sous-système 5 qui supporte la première fonction FEU avec le sous-système 6 sert à la reconfiguration. Si la fonction OBS2 est perdue suite à la défaillance ou la destruction du sous-système 4, le sous-système 5 passe en reconfiguration et supporte partiellement la fonction OBS2 et FEU. La fonction FEU passe donc de l'état "Nominal" à l'état

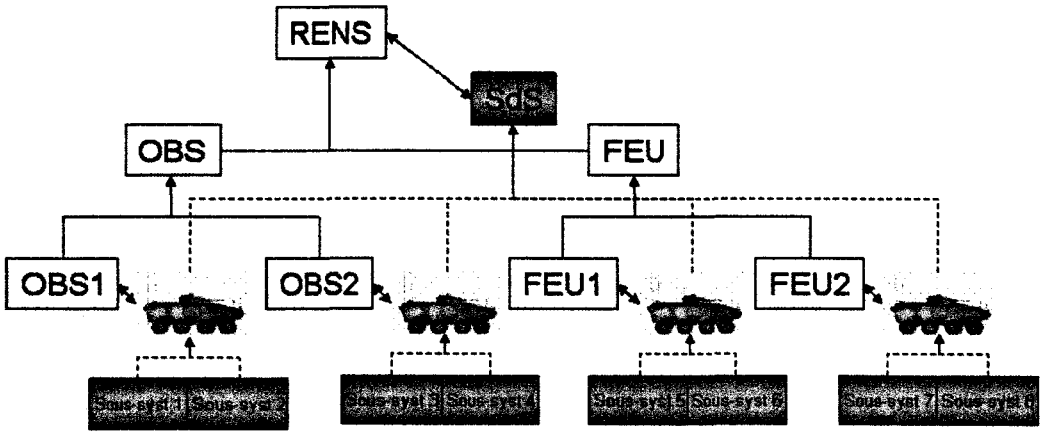

FIG. 5.2 – Exemple d'architecture organico-fonctionnelle de SdS

"Dégradé" et la fonction OBS2 passe de l'état "Panne" à l'état "Dégradé". Le passage à l'état "en reconfiguration" du sous-système 5 dépend donc de l'état du sous-système 4. Cette action de régénération est supposée prendre 15 minutes. Cette valeur correspondant à la durée de reconfiguration n'a pas de caractère réel mais compte tenu de la durée de la mission correspond à un ordre de grandeur réaliste.

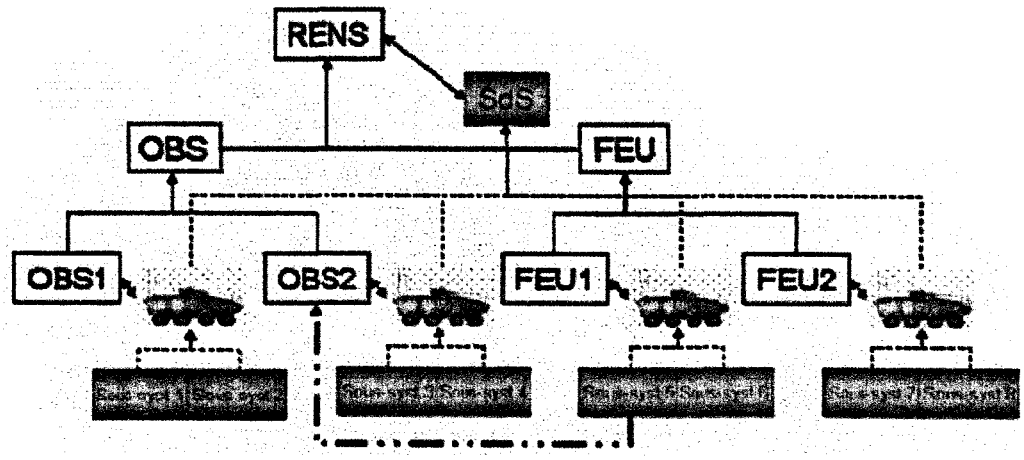

FIG. 5.3 – Solution 1 de reconfiguration : par le sous-système 5 de la plate forme 3.

Scénario 3

Relativement au scénario utilisé dans cette application, il est possible de définir une autre solution de régénération par reconfiguration qui consiste à modifier l'architecture du SdS en introduisant un élément supplémentaire. En effet, comme nous l'avons présenté à la table 5.2, il est possible d'affecter des drônes d'observation aux plates formes. Dans notre exemple, on affecte donc un drone à la plate-forme 3 qui est une plate-forme de feu en appui. Ainsi en cas de perte de la fonction OBS_1 ou OBS_2 suite à une agression ou à une défaillance, le drone peut remplir la fonction d'observation et garantir ainsi la poursuite de la mission. Cette possibilité de régénération est représentée à la figure 5.4. Elle va donc nous permettre de mettre en évidence l'impact de l'architecture sur les possibilités de régénération. Compte tenu de la mission considérée, de sa durée et

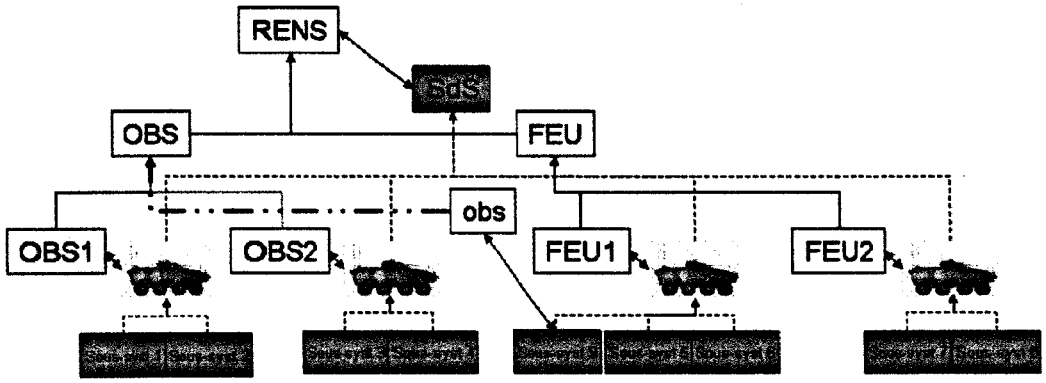

FIG. 5.4 – Solution 2 de reconfiguration : par un drone d'observation affecté à la plate forme 3.

du nombre de plates-formes considérées, il n'y a pas d'autre solution de régénération envisagée.

Relativement à la méthodologie proposée, avant de pouvoir évaluer la disponibilité opérationnelle de l'architecture présentée, les connaissances nécessaires à la construction du modèle dynamique simulable doivent être formalisées.

5.4 Construction du modèle structurel de l'Elément de Manoeuvre RENSEIGNEMENT

Sur la base des descriptions textuelles de l'élément de manoeuvre de renseignement considéré dans cette application, la mise en oeuvre de la méthodologie va nous permettre de construire le modèle support aux évaluations de la disponibilité opérationnelle pour chacune des alternatives retenues. La première étape (cf. figure 3.6), permet de formaliser la connaissance sur le système et les scénarios opérationnels par le biais de la construction du modèle structurel correspondant. Aussi, les règles de construction du

modèle structurel décrites par les différents diagrammes de classe vont nous permettre d'identifer les différents éléments du système indispensables à l'évaluation. En ce sens, la description sera complétée par des données non définies dans la description initiale du scénario et qui font notamment appel à des connaissances métier pour les aspects de fiabilité et de vulnérabilité. Ainsi, le modèle structurel participe à la complétude des modèles en amenant la personne en charge de la modélisation à identifer des relations entre les éléments du système qui ne sont pas nécessairement mentionnés a priori.

Le modèle structurel nous apporte une formalisation de la connaissance sur le système par le bias de la construction de tables de données dans le respect des diagrammes de classe représentatifs des différentes relations à la base du modèle structurel. Ainsi, dans le cadre du développement d'un outil intégré support de l'ingénierie de régénération, les diagrammes de classe constitueraient le support à la construction d'une base de données dans laquelle l'ensemble de la connaissance nécessaire à la construction du modèle dynamique serait regroupée. Ce passage entre les modèles UML conceptuels et les modèles logiques de données correspond à un mécanisme de *dérivation* appliqué aux diagrammes de classe. Nous allons donc dans la suite présenter l'ensemble des tables définies à partir des différents diagrammes de classe, correspondant au cas d'application. A chaque classe est associée une table dont les champs correspondent aux attributs de la classe, les éléments de la table correspondent aux objets de la classe. Pour les associations, qui définissent une relation particulière entre des objects particuliers, des tables sont également définies. Les éléments de ces tables correspondent aux relations identifiées et les champs de la table rappellent les objets concernés. Dans le cadre de notre exemple la *dérivation* a été réalisée manuellement[9].

5.4.1 Les relations de décomposition

La décomposition fonctionnelle

Le premier type de relations défini dans le modèle structurel correspond aux relations de décomposition. Dans le respect du développement du modèle structurel présenté au chapitre III, nous allons tout d'abord présenter la décomposition fonctionnelle sur la base du diagramme de classe de la figure 3.8. Aussi, par rapport au diagramme proposé à titre d'exemple à la figure 3.13, un niveau supplémentaire de décomposition est introduit. La décomposition compte donc trois niveaux :

1. Capacité opérationnelle globale (relative à l'élément de manoeuvre)
2. Capacité opérationnelle (relative aux 2 ensembles de plates-formes : Observation et Feu)
3. Fonction principale (relative à chaque plate-forme)

Comme chaque fonction principale n'appartient qu'à une seule capacité opérationnelle et que toutes les capacités opérationnelles appartiennent à la même capacité opérationnelle globale, capacité opérationnelle et capacité opérationnelle globale sont représentées

[9]Il est cependant à noter que certains ateliers de génie logiciel permettent d'automatiser, dans une certaine mesure, la dérivation.

comme des attributs des fonctions principales dans la table correspondante. La décomposition fonctionnelle est donc représentée à la table 5.5. Enfin, comme le propose le

TAB. 5.5 – Décomposition fonctionnelle de l'exemple

Fonction principale	**Capacité opérationnelle**	**Capacité opérationnelle globale**
OBS_1	OBSERVATION	RENSEIGNEMENT
OBS_2	OBSERVATION	RENSEIGNEMENT
FEU	FEU	RENSEIGNEMENT
FEU_2	FEU	RENSEIGNEMENT

diagramme de la figure 3.13, nous donnerons pour la fonction OBS_1 la table correspondant à la définition de l'état de la fonction. Aussi, à chaque couple fonction-état est associé un niveau de performance[10]. L'architecture fonctionnelle est maintenant dé-

TAB. 5.6 – Niveau de performance associés à l'état d'une fonction

Fonction principale	**Etat**	**Niveau de performance**
OBS_1	Nominal	100%
OBS_1	Dégradé	80%
OBS_1	Secours	30%
OBS_1	Panne	0%

finie dans le respect du modèle structurel. Il nous faut maintenant définir l'architecture organique par le biais des relations de décomposition organique.

La décomposition organique

Pour définir les relations de décomposition organique, nous construisons les tables correspondant au diagramme de la figure 3.14. Nous avons directement introduit tous les constituants qui seront considérés dans les modèles dynamiques relativement aux 3 scénarios de régénération. Dans le respect de la classe constituant de la figure 3.14, les taux de défaillance de chacun des constituants figurent dans la table de décomposition organique. Pour terminer la décomposition organique, le modèle structurel comporte une table supplémentaire définie dans le diagramme de classe qui détermine les états des constituants. Cette table permet de définir les états possibles pour les constituants en leur associant un niveau de performance fonctionnel et un niveau de performance technique qui décrivent les états. Nous donnons, pour illustrer cette partie, la table 5.8 correspondant aux constituants SSYST_1 et SSYST_5.

[10]Les niveaux de performance sont définis relativement à la fonction attendue : par exemple l'observation permet l'observation de jour et de nuit, la perte des équipements supports de l'observation de nuit correspondra à l'état dégradé de la fonction.

TAB. 5.7 – Décomposition organique de l'exemple

Constituant		**Plate-forme**		**EM**		**SdS**
Nom	λ^{11}	Nom	Cat.	Nom	Fonction	Nom
SSYST_1	5.0E-4	VBCI_1	Leger	RENS	Renseignement	SGTIA
SSYST_2	2.0E-5	VBCI_1	Leger	RENS	Renseignement	SGTIA
SSYST_3	5.0E-4	VBCI_2	Leger	RENS	Renseignement	SGTIA
SSYST_4	2.0E-5	VBCI_2	Leger	RENS	Renseignement	SGTIA
SSYST_5	1.0E-6	VBCI_3	Leger	RENS	Renseignement	SGTIA
SSYST_6	2.0E-6	VBCI_3	Leger	RENS	Renseignement	SGTIA
SSYST_9	2.0E-6	VBCI_3	Leger	RENS	Renseignement	SGTIA
SSYST_7	1.0E-6	VBCI_4	Leger	RENS	Renseignement	SGTIA
SSYST_8	2.0E-6	VBCI_4	Leger	RENS	Renseignement	SGTIA

A travers cette table, le modèle structurel nous permet de prendre en compte plusieurs aspects caractérisant les constituants et le scénario opérationnel. En effet, pour remplir correctement la table, il est nécessaire de caractériser les états possibles des constituants par les niveaux de performances fonctionnelles et techniques correspondants. La constitution de cette table s'appuie donc sur des études de vulnérabilité qui ont quant à elles pour objectif de caractériser les composants face aux agressions. Cette caractérisation est à ce niveau relativement générique, la prise en compte spécifique des agressions particulières au niveau de la vulnérabilité intervenant plus tard avec les probabilités liant constituants et agressions. Par ailleurs, étant donné les alternatives de régénération considérées (pas de réparations possibles ni d'échanges, les états *régénéré_1* et *régénéré_2* ne seront pas considérés (mention "/" dans la table). Enfin, la caractérisation de l'état *en reconfiguration* nous permet de montrer l'impact de la reconfiguration sur les performances de la fonction principale du constituant : s'il est utilisé en reconfiguration, le constituant SSYST_5 participe toujours à la fonction FEU mais les performances de la fonction seront dégradées.

La décomposition opérationnelle

Les dernières relations de décomposition concernent la décomposition opérationnelle qui permet de définir la structure de la mission (cf. figure 3.15). Le diagramme de classe définissant les relations de décomposition opérationnelle nous permet de décrire la mission ainsi que ses différents paramètres et, notamment, les agressions potentielles liées à la mission. Compte tenu de la structure du diagramme, nous définissons tout d'abord la table relative aux classes : mission, phase et séquence. Une seconde table caractérisera les agressions et, enfin, une troisième table permettra de représenter l'association des agressions aux séquences. Le scénario retenu pour illustrer la démarche compte une seule séquence et une seule phase pour la mission. En effet, la mission décrite constitue une

TAB. 5.8 – Définition des états pour les constituants

Constituant	**Etat**	**Performance**	
Nom	Nom	Perf. Fonctionnelle	Perf. Technique
SSYST_1	OK	100%	100%
SSYST_1	Panne	0%	100%
SSYST_1	Détruit	0%	0%
SSYST_1	Détérioré	30%	40%
SSYST_1	Régénéré_1	/	/
SSYST_1	Régénéré_2	/	/
SSYST_1	en reconfiguration	/	/
SSYST_5	OK	100%	100%
SSYST_5	Panne	0%	100%
SSYST_5	Détruit	0%	0%
SSYST_5	Détérioré	30%	40%
SSYST_5	Régénéré_1	/	/
SSYST_5	Régénéré_2	/	/
SSYST_5	en reconfiguration	80%	100%

base suffisante pour la mise en oeuvre de la méthodologie et correspond à la fois à la mission, la phase et la séquence.

TAB. 5.9 – Description de la décomposition opérationnelle

Séquence			**Phase**	**Mission**		
No	Nom	Répartition Temporelle	Nom	Type conflit	Type Opposition	Durée
1	Reconnaître un point	100%	Reconnaître un point	Symétrique	armée moderne	24 heures

Dans l'exemple présenté dans ce chapitre, une seule catégorie d'agression est considérée. Nous allons donc réaliser la table correspondante afin d'illustrer comment la classe permet de formaliser les données relatives à l'agression. Les données relatives à l'agression du scénario sont représentées à la table 5.10.

L'association des agressions aux séquences peut donc maintenant être formalisée par le biais d'une table qui met en correspondance les numéros de séquence avec les numéros d'agression. Notre cas d'application ne comptant qu'une séquence et qu'une agression la table ne comportera qu'une ligne (table 5.11).

A travers cet exemple de scénario opérationnel, nous avons illustré la construction d'un modèle structurel particulier, pour la partie concernant les relations de décomposi-

TAB. 5.10 – Table correspondant à la classe agression

No	Catégorie	Probabilité d'occurrence
1	Missiles AC[12]	0.8

TAB. 5.11 – Association Séquence - Agression

Séquence	Agression
1	1

tion dans le respect des règles de construction définies par les différents diagrammes de classe.

5.4.2 Les relations d'interaction

La définition des tables correspondant à la formalisation des données relatives aux relations de décomposition dans le respect des diagrammes de classe donne les principes de construction du modèle de données. Ces principes sont les mêmes quelles que soient les relations considérées. Le scénario choisi pour illustrer la démarche ne comporte pas de relations d'interaction telles qu'elles ont été définies au chapitre III, section 3.3.4[13].

5.4.3 Les relations de contribution

Contribution des fonctions à la mission

Pour terminer la formalisation des connaissances par la construction du modèle structurel, nous allons aborder les relations de contribution. Le premier type de relations de contribution défini par le modèle structurel au chapitre III correspond à la contribution des fonctions à la mission. Cette relation de contribution est définie par le diagramme de classe de la figure 3.20. L'association des fonctions aux séquences de la mission est définie par la classe association "participe" qui caractérise la contribution des fonctions à la séquence. Cette classe association nous permet de construire la table 5.12 qui structure les connaissances des relations de contribution des fonctions aux séquences. La flexibilité constitue, dans le cas où elle est connue, une source de connaissance pour la définition des variables de performance représentatives de la disponibilité opérationnelle : la perte d'une fonction souhaitable n'aura pas le même impact que la perte d'une fonction primordiale.

[13]Le caractère démonstratif de ce cas d'application ne nous impose pas de considérer l'ensemble des relations qu'il est possible de représenter. L'objectif ici étant de montrer la faisabilité de l'approche à travers quelques points particuliers représentatifs des possibilités de modélisation.

TAB. 5.12 – Caractéristiques de la contribution des fonctions aux séquences

Séquence		**Fonction opération-nelle**	**Participe**		
Nom	Répartition Temporelle	Nom	Flexibilité	état début	état fin
Reconnaître un point	100%	OBS_1	Primordiale	OK	Dégradé
		OBS_2	Primordiale	OK	Dégradé
		FEU	Primordiale	OK	Dégradé
		FEU_2	Primordiale	OK	Dégradé

Contribution des constituants aux fonctions

Une fois la contribution des fonctions aux séquences définie, nous pouvons aborder la contribution des constituants aux fonctions telle que définie dans l'architecture organico-fonctionnelle présentée à la figure 5.2. Cette contribution va permettre de mettre en évidence les liens existant entre organes et fonctions pour l'ensemble de l'architecture. Aussi, chaque association reliant une classe de la décomposition fonctionnelle à une classe de la décomposition organique dans le diagramme de classe de la figure 3.21 va donc se traduire par une table représentative des relations de contribution. Étant donné le nombre d'éléments intervenant dans notre architecture, nous présenterons une seule table en spécifiant les différentes relations de contribution (table 5.13). Dans cette table, on retrouve la notion de fonctions principales supportées par les constituants, les plates-formes participent aux capacités opérationnelles et l'élément de manoeuvre qui constitue le SGTIA supporte la capacité opérationnelle globale. Ces relations permettent d'identifier tous les constituants supports de chacune des fonctions principales pour la définition des règles d'agrégation dans le modèle dynamique.

Contribution de la mission aux constituants

La contribution suivante à définir, relativement à la construction du modèle structurel, concerne la contribution des agressions aux constituants. Les relations de contribution correspondantes permettent de spécifier les différentes probabilités liées à la vulnérabilité des constituants en fonction du contexte opérationnel. Ces probabilités doivent être fournies par les experts vulnérabilité en charge des études spécifiques de vulnérabilité. La méthodologie permet donc d'intégrer cette connaissance spécifique dans le même processus de modélisation. Pour construire la table représentative des contributions des agressions aux constituants, nous nous appuyons sur la diagramme de classe de la figure 3.22. Étant donné que le scénario retenu pour la modélisation ne comporte qu'une seule agression (cf. table 5.10), seul l'ensemble des probabilités de vulnérabilité figurera dans la table 5.14 (toutes ces probabilités se reportant à la même agression).

TAB. 5.13 – Représentation de l'architecture organico-fonctionnelle par les relation de contribution des organes aux fonctions

Niveau	**organe**	**Fonction**
SdS	SGTIA	RENSEIGNEMENT
EM	RENS	RENSEIGNEMENT
Plate-forme	VBCI 1	OBS
Plate-forme	VBCI 2	OBS
Plate-forme	VBCI 3	FEU
Plate-forme	VBCI 4	FEU
Constituant	SSYST_1	OBS_1
Constituant	SSYST_2	OBS_1
Constituant	SSYST_3	OBS_2
Constituant	SSYST_4	OBS_2
Constituant	SSYST_5	FEU
Constituant	SSYST_6	FEU
Constituant	SSYST_9	FEU
Constituant	SSYST_7	FEU_2
Constituant	SSYST_8	FEU_2

La description du scénario opérationnel à laquelle s'ajoute les études de vulnérabilité constitue donc les informations à la base de la construction de cette table. On peut notamment remarquer que les probabilités d'atteinte des constituants des VBCI d'observation sont plus grandes car ils sont plus exposés que les VBCI en appui (cf table 5.4). De plus on considère dans cet exemple que le drone (SSYST_9) ne peut être atteint par la menace considérée. Enfin, les constituants supports des fonctions d'observation sont plus vulnérables que les constituants supports des fonctions feu et ont donc des probabilités de destruction plus élevées.

Contribution de la régénération aux constituants

Pour terminer la construction du modèle structurel il nous reste maintenant à intégrer les possibilités de régénération. La régénération est considérée dans le modèle structurel comme la contribution de la régénération aux constituants. Cette contribution est définie par le diagramme de classe de la figure 3.23.

TAB. 5.14 – Caractéristiques de la contribution des agressions aux constituants : la vulnérabilité

Vulnérabilité				**Constituant**
No	Probabilité atteinte	Probabilité destruction	Probabilité Détérioration	Nom
1	0.24	0.8	0.2	SSYST_1
2	0.24	0.8	0.2	SSYST_2
3	0.24	0.8	0.2	SSYST_3
4	0.24	0.8	0.2	SSYST_4
5	0.01	0.2	0.8	SSYST_5
6	0.01	0.2	0.8	SSYST_6
7	0.01	0.2	0.8	SSYST_7
8	0.01	0.2	0.8	SSYST_8
9	0	/	/	SSYST_9

TAB. 5.15 – Table de contribution de la régénération aux constituants

Reconfiguration										
No	No(a)	No(b)	$\lambda(a)$	Type	état reconfiguré	Csq_Etat_fct_A	Csq_Etat_fct_B	Pers.	Outil.	Délai
1	5	4	1.10E-4[14]	1	panne/détruit	dégradé	dégradé	/	/	15 min.
2	9	1		2	panne/détruit	ok	dégradé	/	/	15 min.
3	9	2		2	panne/détruit	ok	dégradé	/	/	15 min.
4	9	3		2	panne/détruit	ok	dégradé	/	/	15 min.
5	9	4		2	panne/détruit	ok	dégradé	/	/	15 min.

L'ensemble des éléments qui caractérisent les différentes solutions de régénération relatives à l'exemple est reporté à la table 5.15. La reconfiguration numéro 1 correspond au scénario 2 de régénération selon lequel le constituant 5 entre en reconfiguration si le composant 4 est détruit ou en panne. La reconfiguration prend 15 minutes et ne nécessite ni personnel ni outillage. Les solutions 2, 3, 4 et 5 correspondent à l'architecture qui comporte un constituant supplémentaire qui servira à la reconfiguration. Aussi, ce constituant supplémentaire offre plus de flexibilité dans la reconfiguration et peut ainsi participer à l'une ou l'autre des fonctions d'observation en reconfigurant un des 4 constituants. Il s'agit d'autre part dans ce cas d'une régénération de type 2 car en effet, l'utilisation du constituant SSYST_9 en reconfiguration n'a pas d'influence sur la la fonction FEU à laquelle il participe par conception (cf. table 5.13).

5.4.4 Synthèse de la construction du modèle structurel

Le modèle structurel correspond donc à une formalisation des connaissances sous la forme de tables représentatives de l'ensemble des relations à la base du modèle structurel. Cette formalisation constitue les bases du développement d'un outil intégré pour l'ingénierie de régénération dont l'ensemble des tables constitue la base de données qui permet la construction du modèle dynamique pour l'évaluation. En effet, un outil qui intégrerait l'ensemble des phases de la méthodologie permettrait la construction automatique du modèle dynamique correspondant à une base de données particulière, dont la structure serait portée par l'outil (cf. §5.4), représentative d'une architecture développée pour un scénario opérationnel particulier dans le respect des mécanismes de construction définis au chapitre IV. Cette partie n'étant pas *encore* réalisée dans nos travaux, nous avons donc présenté les tables correspondant à l'instantiation des différents diagrammes de classe qui constituent les règles de construction du modèle structurel. Aussi, nous allons maintenant construire le modèle dynamique de l'architecture retenue pour illustrer la méthodologie.

5.5 Construction du modèle dynamique de l'Elément de Manoeuvre RENSEIGNEMENT

L'ensemble des tables représentatives du modèle structurel de l'architecture considérée permet d'avoir une description structurée du système (point de vue fonctionnel, point de vue technique) et de son exploitation (point du vue opérationnel). Cette première étape de la méthodologie permet de mettre en forme les connaissances nécessaires à la construction du modèle comportemental pour l'évaluation de la disponibilité opérationnelle. Nous allons dans cette section présenter la construction du modèle dynamique du comportement de l'architecture selon le formalisme des SANs ainsi que l'exploitation du modèle par le biais de simulations de Monte Carlo pour l'estimation de la disponibilité. La construction du modèle dynamique est guidée par les mécanismes de construction introduits au chapitre IV (section 4.1) et suit les différentes étapes de construction liées

à l'outil de modélisation Möbius, déjà présentées au chapitre IV, section 4.2.3. Les mécanismes définissent le paramétrage des différents modèles atomiques des constituants et des fonctions dans le respect des relations identifiées dans le modèle structurel. L'outil Möbius offre la possibilité de développer des modèles dans un environnement de projet nous permettant ainsi de construire une seule application pour l'ensemble de l'architecture dans ses différentes versions et selon les différents scénarios. Aussi, l'ensemble des modèles nécessaires à la représentation des trois scénarios de régénération envisagés est présenté selon qu'il s'agit d'un modèle de constituant ou d'un modèle de fonction.

5.5.1 Construction des modèles atomiques

Pour définir le modèle atomique, les relations de décomposition permettent de définir le nombre et le type de modèles atomiques à construire. Aussi, relativement aux tables 5.7 et 5.5, le modèle dynamique comptera 9 modèles atomiques de constituants et 4 modèles atomiques de fonctions. Par ailleurs, un modèle atomique supplémentaire sera introduit pour la modélisation de l'occurrence des agressions.

Modèle SAN des agressions

Le premier modèle constitutif du modèle dynamique correspond au modèle des agressions. En effet, pour gérer l'occurrence des agressions et le choix de la catégorie d'agression, nous avons introduit un modèle atomique supplémentaire qui détermine, pour l'ensemble des constituants, la catégorie d'agression effective sur l'ensemble des catégories d'agression potentielle pour la mission (cf. tables 5.9 à 5.11), ainsi que le constituant qui sera atteint relativement aux probabilité de la table 5.14. Ce modèle est présenté à la figure 5.5.

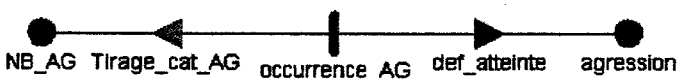

FIG. 5.5 – Modèle SAN des agressions.

La fonction d'entrée de l'*input gate* "Tirage_cat_AG" nous permet de définir un tirage aléatoire dont le résultat déterminera la catégorie d'agression. L'activité temporisée nous permet d'avoir un instant d'occurrence de l'agression qui est uniformément répartie sur l'ensemble de la durée de la mission[15] et enfin, la fonction de l'*output gate* "def_atteinte" définit le marquage de la place "agression" de telle sorte que ce marquage représente le constituant atteint. Pour ce faire, un tirage aléatoire suivant une loi uniforme sur [0, 1] est comparé aux probabilités d'atteinte issues de la table 5.14 représentative de la contribution de la mission aux constituants.

[15]L'instant d'occurrence est déterminé par une loi uniforme sur [1, 24].

Modèles SAN des constituants

Chaque modèle atomique des constituants est construit sur la base du modèle présenté au chapitre IV à la figure 4.4. Les tables représentatives du modèle structurel utilisées au travers des mécanismes de construction définis au chapitre précédent vont nous permettre de spécifier chaque modèle atomique en fonction du constituant qu'il représente.

Tout d'abord, chaque modèle atomique des constituants intègre le taux de défaillance des constituants à partir des données issues de la table de décomposition organique. En effet, les taux de défaillances sont des caractéristiques propres à chaque constituant qui figurent comme attribut de la classe constituant du modèle structurel. Les transitions vers l'état "panne" dans les modèles atomiques SAN de tous les constituants intègrent donc le taux de défaillance du constituant qui figure dans la table 5.7[16].

Le modèle structurel ne comportant pas de relations d'interaction entre les constituants, les premiers mécanismes de construction utilisés pour la définition des modèles SAN des constituants correspondent aux mécanismes dérivés des relations de contribution de la mission aux constituants représentés par les relations $\mathscr{R}_4$ et $\mathscr{R}_5$. Ces relations nous permettent de considérer les vulnérabilités définies dans la table 5.14. Ainsi, pour chaque constituant, les probabilités notées : "probabilité destruction" et "probabilité détérioration" constituent la distribution de probabilités des cas de l'activité relative aux agressions. La figure 5.6 illustre la définition des probabilités relatives à chaque cas pour le constituant SSYST_1. Ainsi, dans le cas d'une mission comportant plusieurs catégories d'agression, les probabilités sont saisies pour chaque catégorie, pour chacun des cas de chaque modèle de constituant.

Les autres mécanismes utilisés pour la construction des différents atomes sont les mécanismes liés à la régénération et donc, plus particulièrement, à la reconfiguration. Le premier mécanisme relatif à la régénération mit en oeuvre dans la modélisation est caractérisé par la relation $\mathscr{R}_9$ définie au chapitre IV. En effet, il existe une relation de reconfiguration telle qu'il existe un taux de défaillance pour le composant qui supporte la reconfiguration : Reconfiguration No 1 dans la table 5.15. Ce taux de défaillance correspond à l'ajout d'un facteur 100 au taux de défaillance intrinsèque du constituant SSYST_5. La relation $\mathscr{R}_9$ nous impose donc de considérer ce taux de défaillance dans la définition de l'activité régissant le passage de l'état "reconfiguration"à l'état "panne" pour le constituant SSYST_5. La considération de ce mécanisme de construction est illustrée à la figure 5.7.

Le second mécanisme lié à la régénération à prendre en compte dans la construction des modèles atomiques SAN des constituants est supporté par la relation $\mathscr{R}_{10}$ qui définit deux éléments à considérer dans la définition de la transition entre l'état "ok" et l'état "reconfiguration" pour les constituants support de la reconfiguration. Le premier élément entrant de la définition de la transition est lié aux états des constituants reconfigurés qui vont entraîner la mise en oeuvre de la reconfiguration (colonne 5 : "état reconfiguré" de la table 5.15). Ces états définissent en partie les conditions de validité de l'activité "en_reconfiguration" des constituants SSYST_5 et SSYST_9. Le mécanisme impose

[16]Le paramétrage d'une activité représentative d'une défaillance a déjà été illustré au chapitre IV à la figure 4.7

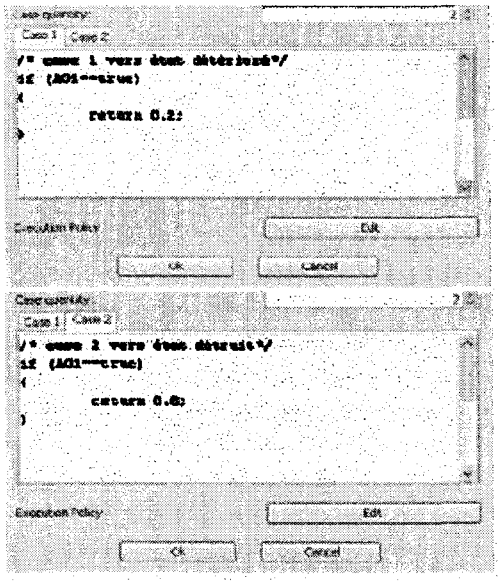

FIG. 5.6 – Définition de la distribution de probabilités des cas pour les états détérioré et détruit

donc de reporter les états correspondant dans les modèles de SSYST_5 et SSYST_9 et de considérer leur marquage dans la fonction d'activation de l'*input gate* liée à l'activité "en_reconfiguration". Par exemple, pour le constituant SSYST_5, la reconfiguration a lieu si le constituant SSYST_4 passe dans l'état "panne" ou dans l'état "détruit" (cf. Reconfiguration No 1 dans la table 5.15). L'expression du mécanisme lié à la relation $\mathscr{R}_{10}$ pour le constituant SSYST_5 est illustré à la figure 5.8 .

Enfin, pour chacune des solutions de reconfiguration, il existe un délai relatif à la mise en oeuvre de la solution de reconfiguration. La prise en compte de ce délai est définie par le mécanisme supporté par la relation $\mathscr{R}_{10}$ relative à la transition vers l'état "reconfiguration" pour le constituant support de la reconfiguration. Les constituants SSYST_5 et SSYST_9 intègrent donc le délai de reconfiguration comme paramètre de l'activité temporisée notée "en_reconfiguration".

L'architecture particulière considérée ne requiert pas l'utilisation de tous les mécanismes de construction définis au chapitre IV pour les constituants. Nous avons cependant illustré l'exploitation des mécanismes à mettre en oeuvre compte tenu des différentes relations définies au niveau du modèle structurel. Nous allons maintenant présenter la construction des modèles atomiques des fonctions.

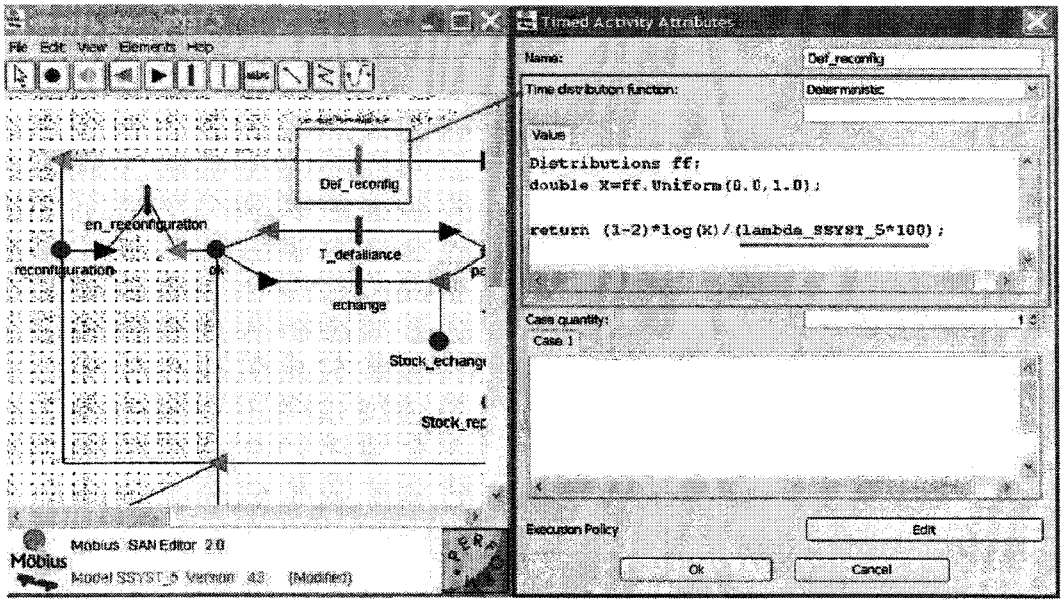

FIG. 5.7 – Prise en compte de l'influence de la reconfiguration sur la fiabilité du constituant SSYST_5

Modèles SAN des fonctions

De la même manière que nous avons appliqué les mécanismes de construction définis au chapitre IV pour construire les modèles atomiques SAN des constituants sur la bases des tables représentatives du modèle structurel, nous détaillons la construction des modèles atomiques des fonctions de l'architecture. Pour rendre compte des différents scénarios et notamment des différentes possibilités de reconfiguration nous avons créé 2 modèles pour les fonctions OBS_1 et OBS_2 pour prendre en compte la reconfiguration par le drone.

Vu la taille et la structure de l'architecture retenue, aucune interaction fonctionnelle n'a été identifiée. Le mécanisme supporté par les relations de type $\mathscr{R}_{11}$ ne sera donc pas utilisé. Le premier mécanisme mis en oeuvre pour la construction des modèles atomiques des fonctions relève des règles d'agrégation qui permettent de déterminer l'état de la fonction en fonction de l'état de ses constituants supports. Ces règles sont basées sur l'exploitation des relations de contribution des constituants aux fonctions. Pour illustrer ce mécanisme nous développerons la construction du modèle de la fonction OBS_1 sur la base des relations de contribution des constituants à la fonctions OBS_1 résumée dans le table 5.13. Le mécanisme lié aux contributions des constituants aux fonctions est supporté par la relation $\mathscr{R}_{12}$ qui impose de considérer l'état des constituants dans la définition des changements d'état des fonctions. Ce principe déjà illustré au chapitre IV section 4.6, nous permet de définir les conditions sur les états des constituants pour que la

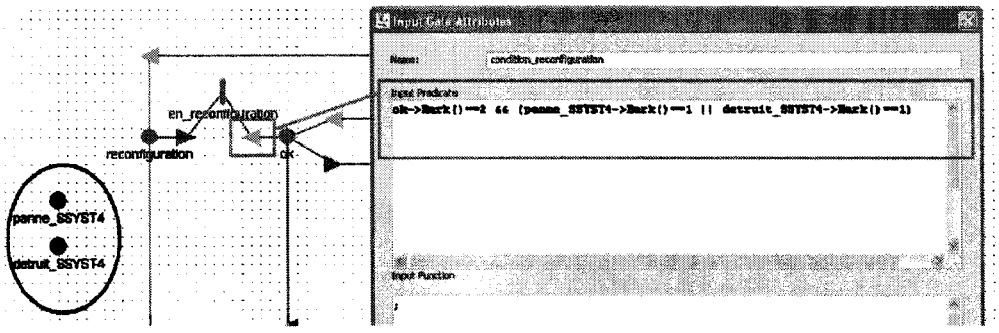

FIG. 5.8 – Prise en compte du mécanisme de construction $\mathscr{R}_{10}$ dans le modèle de SSYST_5

fonction change d'état. Pour mettre en oeuvre les solutions de régénération définies dans notre application, nous avons déjà abordé dans les modèles de constituants les différents états qu'il fallait introduire au niveau des constituants supports de la reconfiguration. De la même manière, la reconfiguration s'exprime également au niveau des modèles atomiques des fonctions. Aussi, nous donnons dans ce chapitre un exemple d'utilisation de ce mécanisme relativement au scénario 2 de régénération selon lequel, le constituant SSYST_5 permet de reconfigurer la fonction OBS_2 en se subsituant au constituant SSYST_4 en cas de panne ou de destruction. Nous avons déjà illustré l'impact de cette solution sur la modélisation du constituant SSYST_5. Nous développons maintenant l'impact sur le modèle des fonctions OBS_2 et FEU respectivement supportées en partie par les constituants SSYST_4 et SSYST_5.

Pour la fonction FEU, la reconfiguration fait passer la fonction de l'état "ok" à l'état "dégradé" (le constituant SSYST_5 n'étant plus dans un état nominal, cf. table 5.8). Cette condition se retrouve donc dans l'*input gate* en amont de l'activité qui représente la transition de l'état "ok" à l'état "dégradé". Cette condition va donc dépendre du marquage de la place représentant l'état "en_reconfiguration" du constituant SSYST_5 tel que défini par la relation $\mathscr{R}_{13}$. Cette place est repérée dans la figure 5.9 qui correspond au modèle SAN de la fonction FEU.

Pour la fonction OBS_2, la reconfiguration permet de faire passer la fonction de l'état "panne" à l'état "dégradé". L'activité définissant le passage vers l'état "dégradé" depuis les états "panne" ou "secours" doit intégrer l'état "en_reconfiguration" du SYSYT_5. Pour ce faire nous introduisons tout d'abord cet état dans le modèle de la fonction (cf. figure 5.10 dans laquelle l'état de SSYST_5 est repéré).

Le report de la place représentative de l'état "en_reconfiguration" du SSYST_5 dans le modèle de la fonction OBS_2 permet donc de considérer son marquage dans la fonction d'activation de l'*input gate* notée "panne_secours_vers_D" qui définit les conditions de validation de l'activité représentative du passage de la fonction dans l'état "dégradé" à partir de l'état "panne" ou "secours".

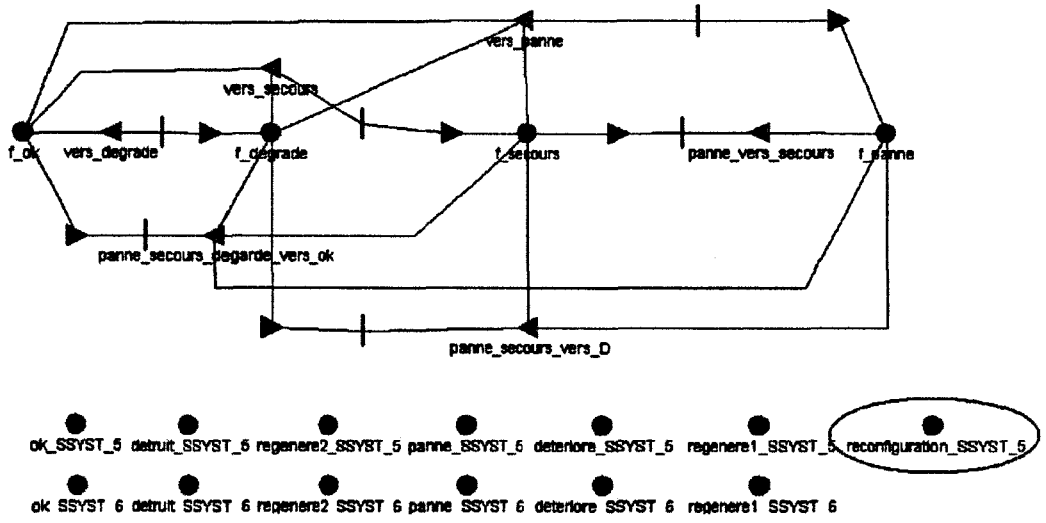

FIG. 5.9 – Modèle SAN de la fonction FEU pour la reconfiguration

Les mécanismes de construction des modèles atomiques SAN des fonctions qu'il était possible de mettre en oeuvre relativement au modèle structurel de l'architecture ont été présentés. Des exemples de fonctions d'activation des *input gates* ont été donnés de manière à illustrer les règles d'agrégation. La définition de ces règles fait donc appel à une connaissance experte sur les différentes fonctions qui regroupe les résultats des études de sûreté de fonctionnement pour la prise en compte de l'impact des états "panne" et "régénéré_1" sur l'état de la fonction, ainsi que les résultats des études de vulnérabilité pour l'impact des états "détruit", "détérioré" et "régénéré_2". Le comportement des fonctions peut donc ainsi être complètement défini par l'écriture des équations du marquage des places représentatives des états des constituants dans les fonctions d'activations des différentes *input gates* des modèles SAN des fonctions.

La seconde étape dans le construction des modèles SAN consiste en la construction du modèle composé (cf. section 4.2.3 au chapitre IV). La section suivante détaille donc les modèles composés représentatifs de l'architecture retenue ainsi que des différents scénarios de régénération.

5.5.2 Construction des modèles composés

Le principe de construction des modèles composés a été présenté au chapitre IV, section 4.2.3. Ce modèle permet en effet de définir les partages de variables d'état pour que les marquages des places identiques soient les mêmes dans tous les modèles. Pour représenter les scénarios de régénération considérés pour l'architecture retenue, deux modèles composés ont été développés. Le premier modèle composé permet de considérer les scénarios 1 et 2 de régénération dans lesquels le constituant SSYST_9 ne participe

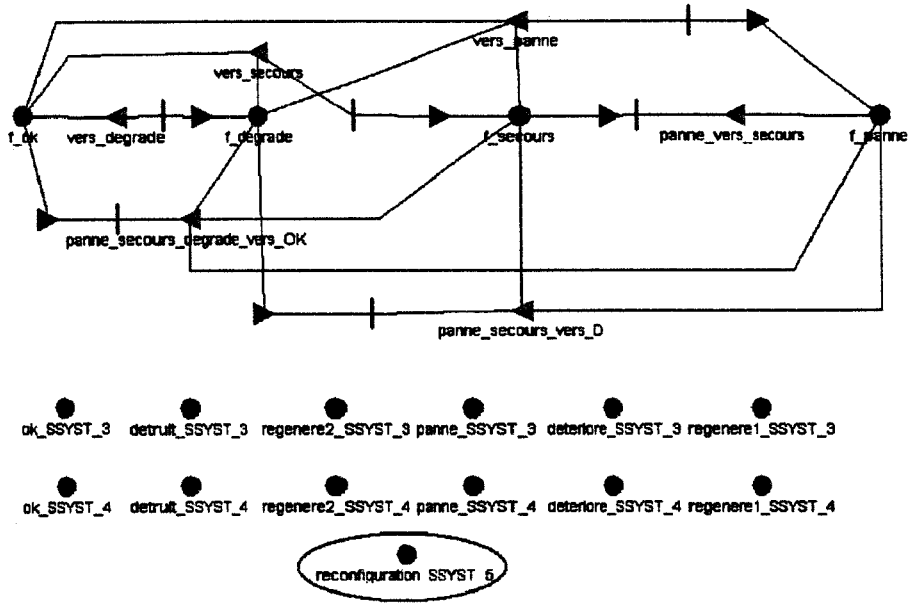

FIG. 5.10 – Modèle SAN de la fonction OBS_2 pour la reconfiguration

pas. Ce premier modèle est représenté à la figure 5.11. Pour illustrer le principe de partage

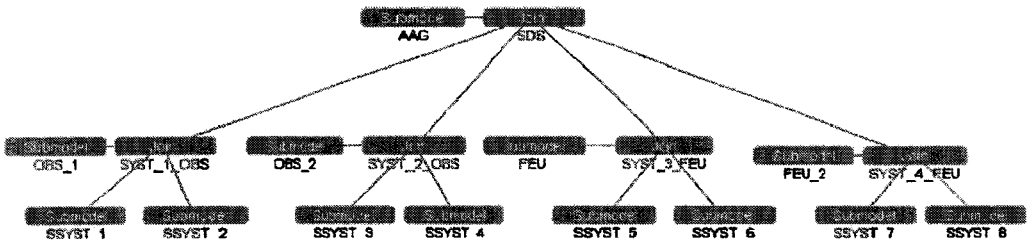

FIG. 5.11 – Modèle composé de l'architecture pour les scénarios 1 et 2 de régénération

de variables d'états, nous donnons dans les tables 5.16 et 5.17 les variables correspondant respectivement aux modèles *Join* notés SYST_1_OBS et SDS.

Dans la table 5.16 sont donc définis tous les partages relatifs au SSYST_1 et SSYST_2 supports de la fonctions OBS_1. On remarque notamment que chaque place représentative d'un état d'un constituant est partagée avec la même place mais appartenant au modèle atomique de la fonction.

La table 5.17 répertorie les partages de variables d'états du modèle de plus haut niveau noté "SDS". La premiere *State Variable* nommée "agression" permet de gérer l'oc-

TAB. 5.16 – Définition des partages de variables d'état pour le *join* modèle du VBCI 1

Join Modèle : SYST_1_OBS

State Variable Name	*Submodel Variables*
agression	SSYST_1->agression
	SSYST_2->agression
deteriore_SSYST_1_F	OBS_1->deteriore_SSYST_1
	SSYST_1->deteriore
deteriore_SSYST_2_F	OBS_1->deteriore_SSYST_2
	SSYST_2->deteriore
detruit_SSYST_1_F	OBS_1->detruit_SSYST_1
	SSYST_1->detruit
detruit_SSYST_2_F	OBS_1->detruit_SSYST_2
	SSYST_2->detruit
ok_SSYST_1_F	OBS_1->ok_SSYST_1
	SSYST_1->ok
ok_SSYST_2_F	OBS_1->ok_SSYST_2
	SSYST_2->ok
panne_SSYST_1_F	OBS_1->panne_SSYST_1
	SSYST_1->panne
panne_SSYST_2_F	OBS_1->panne_SSYST_2
	SSYST_2->panne
regenere1_SSYST_1_F	OBS_1->regenere1_SSYST_1
	SSYST_1->regenere1
regenere1_SSYST_2_F	OBS_1->regenere1_SSYST_2
	SSYST_2->regenere1
regenere2_SSYST_1_F	OBS_1->regenere2_SSYST_1
	SSYST_1->regenere2
regenere2_SSYST_2_F	OBS_1->regenere2_SSYST_2
	SSYST_2->regenere2

TAB. 5.17 – Définition des partages de variables d'état pour le *join* modèle SDS

Join Modèle : SDS

State Variable Name	*Submodel Variables*
agression	SYST_1_OBS->agression
	SYST_2_OBS->agression
	SYST_3_FEU->agression
	SYST_4_FEU->agression
	AAG->agression
detruit_SSYST_4_F	SYST_2_OBS->detruit_SSYST_4_F
	SYST_3_FEU->detruit_SSYST4
panne_SSYST_4_F	SYST_2_OBS->panne_SSYST_4_F
	SYST_3_FEU->panne_SSYST4
reconfiguration_SSYST_5	SYST_2_OBS->reconfiguration_SSYST_5
	SYST_3_FEU->reconfiguration

currence de l'agression pour tous les constituants. Les variables suivantes correspondent à la mise en oeuvre de la reconfiguration pour le scénario 2. Ces trois variables permettent d'assurer la cohérence du marquage des places impliquées dans la reconfiguration.

Pour pouvoir mettre en oeuvre le troisième scénario de régénération, un second modèle composé a été développé, qui intègre le constituant SSYST_9. Ce modèle est représenté à la figure 5.12. Le partage de variables est basé sur le même principe que pour le modèle précédent.

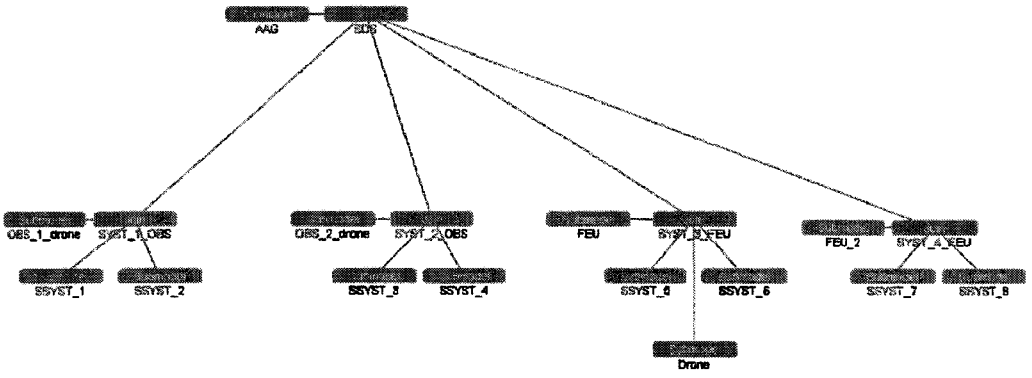

FIG. 5.12 – Modèle composé de l'architecture pour le scénario 3 de régénération

Après la construction des modèles supports aux simulations, les variables de performance doivent être définies. En effet, les variables de performance associées aux modèles atomiques permettent l'évaluation des temps de séjour dans les différentes places des

différents modèles en construisant des taux de récompense associés aux marquages des places.

5.5.3 Définition des variables de performance

Le principe de construction des variables de performance a été défini au chapitre IV aux sections 4.2.2 et 4.2.3. Dans notre application, nous nous intéressons aux performances globales de la fonction de renseignement supportée par les quatre fonctions opérationnelles OBS_1, OBS_2, FEU et FEU_2. Relativement au critère d'évaluation défini à la section 5.3.1, nous construisons une variable de performance représentative de la disponibilité opérationnelle de la fonction renseignement sur la base des performances des quatre fonctions opérationnelles. Pour les fonctions opérationnelles, nous nous basons sur la définition de la survivabilité présentée au chapitre I section 1.3.3 pour définir les états de disponibilité. Une capacité opérationnelle entière sera représentée par l'état "ok" d'une fonction et une capacité opérationnelle correspondra à l'état "dégradé", aussi les fonctions opérationnelles seront considérées comme *disponibles* pour la mission si elles sont dans l'état "ok" ou "dégradé". La variable de performance représentative de la disponibilité opérationnelle de la fonction renseignement est donc construite sur la base de la considération suivante : *la mission sera considérée comme réussie si les deux fonctions d'observation et au moins une des fonctions FEU sont disponibles pendant 95% de la durée de la mission.* La disponibilité de la fonction renseignement peut donc être écrite de la manière suivante :

$$
\begin{aligned}
&Dispo\_RENS = \\
&\Big(\\
&((OBS\_1\_OK \vee OBS\_1\_Degrade) \wedge (OBS\_2\_OK \vee OBS\_2\_Degrade)) \\
&\wedge \\
&((FEU\_OK \vee FEU\_Degrade) \vee (FEU\_2\_OK \vee FEU\_2\_Degrade)) \\
&\Big)
\end{aligned}
$$

Le taux de récompense définissant la variable de récompense va donc normalement dépendre du marquage des places représentatives des états des différentes fonctions. L'outil Möbius permet la construction d'un *modèle de récompense* dans lequel sont définies toutes les variables de récompense. Toutes les données relatives à la variable Dispo_RENS sont reportées dans la table 5.18.

La variable est donc estimée à partir de taux de récompense évalués par la fonction de récompense qui représente les conditions de disponibilité de la fonction renseignement. La variable est calculée sur l'intervalle [0, 24] qui représente la durée de la mission. Möbius offre la possibilité d'estimer directement la distribution de probabilité de la variable moyennant le paramétrage d'une borne inférieure (0), d'une borne supérieure (24) et d'un pas de calcul (0.05). L'intervalle de confiance est également défini pour déterminer la précision de l'estimation.

D'autres variables de performance ont également été introduites pour les différents scénarios considérés dans cette application. Le principe de définition des taux de récom-

TAB. 5.18 – Variable de performance Dispo_RENS

Fonction de récompense		
if (((OBS_1->f_ok->Mark()==1 || OBS_1->f_degrade->Mark()==1) && (OBS_2->f_ok->Mark()==1 || OBS_2->f_degrade->Mark()==1)) && ((FEU->f_ok->Mark()==1 || FEU->f_degrade->Mark()==1) || (FEU_2->f_ok->Mark()==1 || FEU_2->f_degrade->Mark()==1))) return 1 ;		
Statistique des Simulations	Type	Intervalle de temps
	Options	Estimer la moyenne
		Estimer la Distribution
		Niveau de confiance relatif
	Paramètres	Temps début 0.0
		Temps fin 24
	Distributions	Borne inférieure de la distribution 0.0
		Borne supérieure de la distribution 24.0
		Pas d'estimation 0.05
	Précision	Niveau de confiance 0.95
		Intervalle de confiance 0.1

pense étant le même que pour la variable précédemment introduite, nous ne présenterons donc pas l'ensemble des variables.

Nous disposons donc maintenant de tous les éléments nécessaires pour effectuer les simulations afin d'obtenir des estimations des différentes variables et ce pour les trois scénario de régénération envisagés.

5.5.4 Principe des simulations

Pour l'estimation des variables de récompense, nous avons utilisé les fonctionnalités de simulation du logiciel Möbius qui permet l'analyse des modèles par le biais de simulations de Monte Carlo quand une résolution analytique n'est pas permise. Pour chaque simulation, on spécifie le nombre de run maximum (*maximum batches*) ainsi que la séquence d'initialisation du générateur de nombre aléatoire (*random number seed*). La connaissance de la séquence d'initialisation permet de réaliser exactement les mêmes histoires si la séquence est inchangée ou, à l'inverse, de modifier l'initialisation pour vérifier la convergence des estimations. Les simulations sont basées sur un simulateur à événements discrets, utilisant soit un générateur aléatoire de Fibonacci soit un générateur Tausworthe (A. Williamson 1998). Ces générateurs largement traités dans la littérature, (P. L'Ecuyer 1996) ne seront pas abordés plus en détail.

Pour une meilleure lisibilité des résultats, nous avons choisi de tracer pour chaque scénario la courbe représentant *1-Fonction de répartition de Dispo_RENS* en fonction du temps. Cette courbe représente donc à chaque instant la probabilité que le temps moyen de bon fonctionnement soit supérieur à t. On peut donc directement avoir accès par lecture sur la courbe à la probabilité de réussite de la mission. La valeur moyenne de Dispo_RENS sera également évaluée et en fonction des éléments caractéristiques des scénarios étudiés, d'autres variables pourront être introduites. Les résultats des différents scénarios proposés sont exposés dans la suite.

Scénario n°1

Dans le premier scénario considéré, le modèle est paramétré de manière à ce qu'aucune agression ne se produise et il n'y a pas de régénération.
La courbe obtenue pour le scénario représentant *1-Fonction de répartition de Dispo_RENS* est donnée à la figure 5.13. Cette courbe a été obtenue avec les paramètres suivants :

- horizon de simulation : 24 heures
- pas d'observation : 0.05 heure
- séquence d'initialisation : 31415
- nombre de run effectués N=10146000 (pour un temps de calcul de 519,847 secondes).[17]

[17]Le nombre de run effectué correspond au nombre minimum de run pour lequel tous les intervalles de confiance des différentes variables sont satisfaits. Le nombre maximum de run autorisé a été fixé pour toutes les simulation tel que $1000 \leq N \leq 100000000$ de sorte que le critère d'arrêt soit préférentiellement lié aux intervalles de confiance pour assurer la précision des résultats.

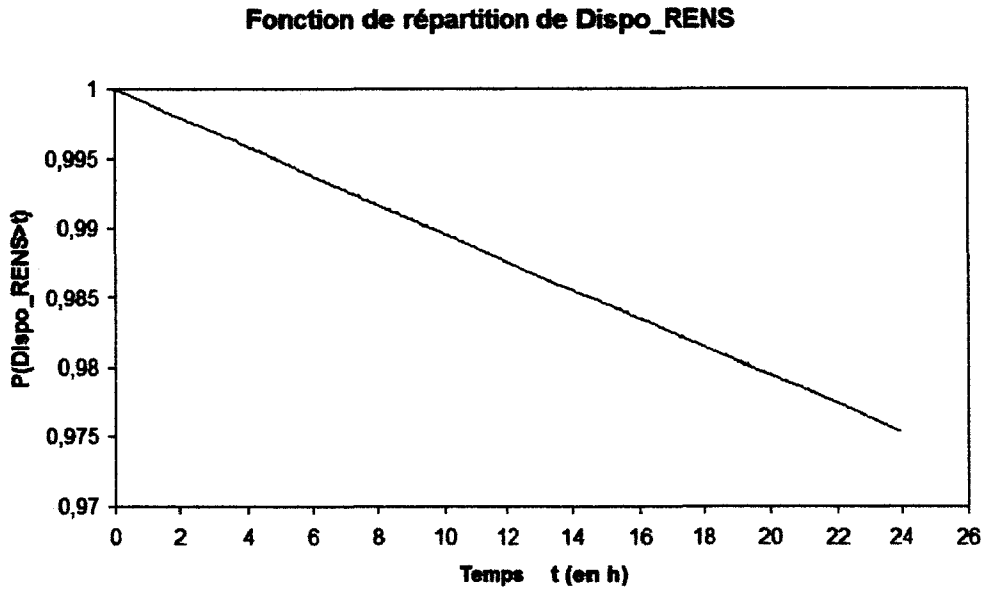

FIG. 5.13 – Fonction de répartition de la variable Dispo_RENS en présence de défaillance uniquement

La probabilité de réussite de la mission correspondante est :
$P(Dispo\_RENS > 22.8) = 0.9765$, [0.9764, 0.9766].
Le temps moyen de bon fonctionnement correspondant est de 23.70 +/- 0.001 (en heures) soit une disponibilité opérationnelle moyenne[18] de 0.987. Les simulations offrent donc une bonne précision des résultats avec un intervalle de confiance supérieur à l'intervalle spécifié compte tenu du nombre de run effectués. De plus, ce scénario est particulièrement intéressant dans la mesure où la seule présence de défaillance et l'absence de régénération rendent compte de la fiabilité du système. En effet, si l'état global de l'architecture représenté par la variable Dispo_RENS n'est plus vrai, l'absence de régénération ne permet pas de retrouver d'autres états fonctionnels. La mesure de disponibilité devient alors une mesure de fiabilité. Aussi, en évaluant la variable Dispo_RENS non plus sur un intervalle de temps mais à un instant donné, nous pourrons comparer la valeur obtenue par simulation avec la valeur obtenue par calcul. La mission durant 24 heures nous évaluerons la variable à t=24 heures. Ainsi, dans la même simulation (séquence d'initialisation : 31415) nous avons défini une variable Fiab_RENS évaluée à l'instant $t = 24$. Nous avons obtenu les résultats suivants :
$Fiab\_RENS(24) = 0.9753$ avec l'intervalle de confiance à 95% $+/- 0.00009$.
Compte tenu que les défaillances suivent une loi exponentielle à taux λ constant et que

[18] La disponibilité opérationnelle moyenne est obtenue par le rapport : $\frac{\text{Temps moyen de bon fonctionnement}}{\text{durée mission}}$

les équations qui déterminent l'état des fonctions à partir des états des composants sont des équations combinatoires et que la variable Fiab_RENS est identique à la variable Dispo_RENS également déterminée sur la base d'une équation logique, nous allons également calculer la fiabilité à t=24 heures sur la base de la représentation par un arbre de défaillance de la fonction Renseignement. L'arbre de défaillance correspondant à l'architecture modélisée pour les simulations est donné à la figure 5.14. La fiabilité de chaque

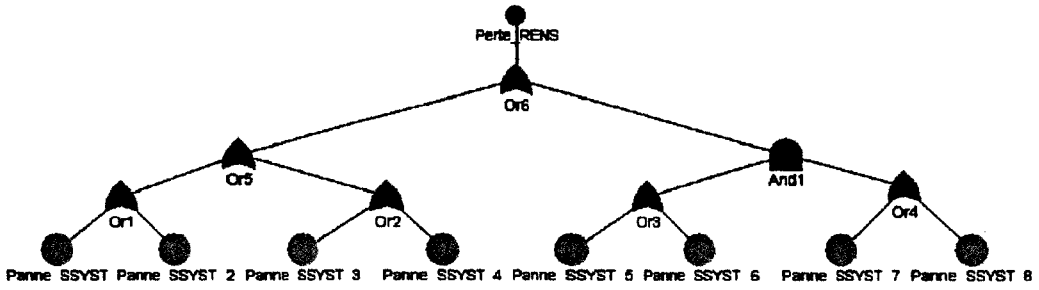

FIG. 5.14 – Arbre de défaillance correspondant à l'architecture simulée

constituant est rappelée ci-dessous : $R_{SSYST\_i}(t) = exp(-\lambda_i.t)$. On obtient donc pour la fiabilité globale du système de renseignement :

$$R_{RENS}(t) = [exp(-(\lambda_1+\lambda_2+\lambda_3+\lambda_4).t)].[1-((1-(exp((\lambda_5+\lambda_6).t))).(1-(exp((\lambda_7+\lambda_8).t))))]$$

En associant les taux de défaillance de chaque constituant définis à la table 5.7 on obtient numériquement[19] pour $t = 24$: $R_{RENS}(24) = 0.9753$. L'erreur relative de calcul due à la simulation est de l'ordre de $6E-005\%$. Ces résultats nous permettent donc de conclure quant à la précision fournie par les simulations. Sur un exemple simple, l'erreur commise par simulation est négligeable devant les grandeurs évaluées. Par ailleurs, ce calcul nous permet également de valider partiellement le modèle dans le sens où, pour la partie du comportement relatif aux défaillances, le comportement simulé fournit des résultats sensiblement égaux aux résultats obtenus analytiquement.

La deuxième partie de ce scénario vise à montrer l'impact des agressions et donc des dommages sur la disponibilité opérationnelle en supposant l'occurrence de l'agression pendant la mission. L'architecture est supposée ne comporter aucune possibilité de régénération. La variable Dispo_RENS a été obtenue relativement aux paramètres de simulation suivants :

- horizon de simulation : 24 heures
- pas d'observation : 0.05 heure
- nombre de run effectués N=215000 (pour un temps de calcul de 15.352 secondes).

La fonction de répartition pour la disponibilité (variable Dispo_RENS) est donnée par la figure 5.15. La distribution uniforme du temps d'occurrence de l'agression est très nette sur la fonction de répartition de la disponibilité qui décroît de manière quasi

[19]Calcul effectué sous *MATLAB*®

linéaire. Dans ces conditions, la probabilité de réussite de la mission est :

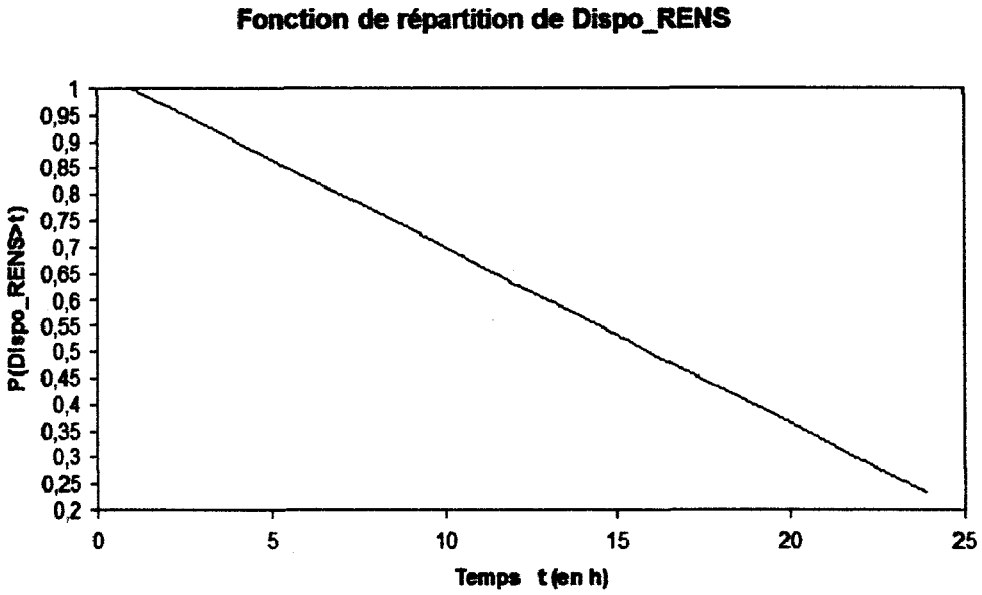

FIG. 5.15 – Fonction de répartition de la variable Dispo_RENS en présence d'une agression sans régénération

$P(Dispo\_RENS > 22.8) = 0.2713$, [0.2694, 0.2732]
Le temps moyen de bon fonctionnement pour l'architecture est alors de 15.15 +/- 0.03 (en heures) soit une disponibilité opérationnelle moyenne du SdS de 0.6313.
Ce scénario met donc en évidence l'importance de la prise en compte des agressions et des dommages dans l'évaluation de la disponibilité opérationnelle au combat, compte tenu de leurs probabilités d'occurrence au regard des taux de défaillance des constituants. Dans de tels contextes, la régénération revêt un caractère indispensable pour garantir la disponibilité opérationnelle des matériels et minimiser les échecs de mission dus à une indisponibilité.

La problématique de la régénération va maintenant être abordée relativement au scénario 2 dans lequel l'architecture possède une possibilité de reconfiguration.

Scenario n°2

L'objectif de ce scenario est de mettre en évidence l'effet de la reconfiguration sur la disponibilité opérationnelle mais également de montrer comment la reconfiguration peut avoir une influence sur la fiabilité des constituants. Afin de mieux comprendre l'effet de la

reconfiguration et son influence sur la fiabilité, trois autres variables seront commentées relativement à ce scénario :

- le temps moyen passé en reconfiguration pour le constituant SSYST_5,
- le temps moyen passé en panne pour ce même constituant,
- le temps moyen passé en panne pour la fonction FEU.

Étant donné les intervalles de confiance, le nombre de runs effectués a été de 199000 pour un temps de simulation de 15,652 secondes. La fonction de répartition de la variable Dispo_RENS est représentée à la figure 5.16. Le premier effet notoire de la reconfiguration est donc d'augmenter la probabilité de réussite de la mission :
$P(Dispo\_RENS > 22.8) = 0.3715$, [0.3714, 0.3717]
Le temps moyen passé en reconfiguration pour le constituant SSYST_5 correspondant est de $1.286 + / - 0.001$ heures.
Le temps moyen de bon fonctionnement donné par la variable Dispo_RENS correspondant à ce scénario est de : 16.30 +/- 0.002 (en heures).
La disponibilité opérationnelle moyenne passe de 0.6313 sans reconfiguration à 0.6795 avec la reconfiguration. La probabilité de réussite de la mission passe quant à elle de 0.2713 à 0.3715.

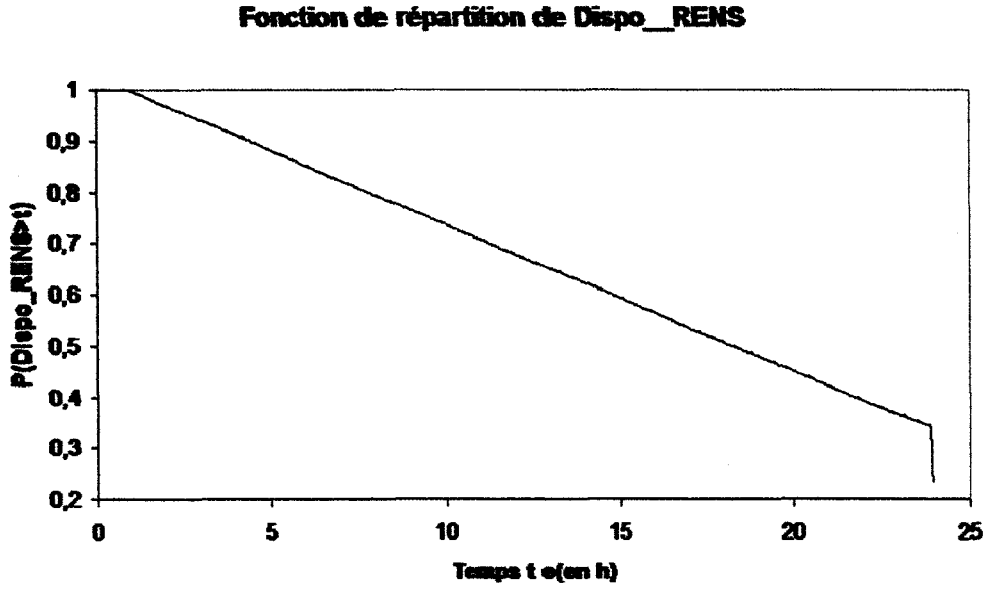

FIG. 5.16 – Fonction de répartition de la variable Dispo_RENS en présence d'une agression et de régénération : reconfiguration par le constituant SSYST_5

Dans ces conditions de fonctionnement, le taux de défaillance du constituant SSYST_5 est le même quel que soit son état, le temps moyen passé dans l'état "panne" pour le

constituant SSYST_5 relatif à cette simulation est alors de : $0.0002 + / - 0.00002$ (en heures). Pour la fonction FEU supportée par les constituants SSYST_5 et SSYST_6, le temps de séjour dans l'état "panne" exprimé en heures vaut $0.04 + / - 0.0002$.

Pour montrer l'effet de la reconfiguration sur la fiabilité du constituant, on considère que le taux de défaillance est multiplié par 100 si le constituant est dans l'état "en_reconfiguration". Dans ces conditions, on obtient les temps de séjour dans l'état panne suivant :
SSYST_5 : $0.001 + / - 0.0001$
fonction FEU : $0.042 + / - 0.0006$
Étant donné les ordres de grandeur entre les taux de défaillance et la durée de la mission, la différence avec la simulation précédente est faible mais correspond à une augmentation de 4% du temps de séjour dans l'état panne pour la fonction FEU.

Le troisième scénario envisagé propose une solution de régénération toujours basée sur la reconfiguration mais avec une architecture différente.

Scénario 3

Une autre solution de régénération est envisagée et consiste à affecter un drone à la troisième plate-forme. Ce drone est supposé pouvoir reconfigurer indifféremment les fonctions OBS_1 ou OBS_2, en se substituant au premier constituant perdu pour l'une ou l'autre des fonctions. Le drone reconfigure donc indifféremment les constituants SSYST_1, SSYST_2, SSYST_3, SSYST_4 (cf. table 5.15), mais il ne peut se substituer qu'à un seul à la fois. La fonction de répartition obtenue pour la variable Dispo_RENS dans ces conditions est donnée à la figure 5.17. La simulation a compté 405000 runs pour un temps de simulation de 38.265 secondes. La probabilité de réussite de la mission avec cette solution de reconfiguration est de :
$P(Dispo\_RENS > 22.8) = 0.8509$, [0.8498, 0.8520]
Le temps moyen de bon fonctionnement de l'architecture correspondant est alors de : $22.16 + / - 0.015$ (en heures), soit une disponibilité opérationnelle moyenne de 0.9235. Le temps moyen passé en reconfiguration pour le drone (SSYST_9) correspond à environ 30% du temps de la mission, soit une moyenne de $7.219 + / - 0.0238$ heures. La reconfiguration est globalement répartie de manière équivalente sur OBS_1 et OBS_2 avec des temps de séjour moyen dans l'état "dégradé" respectivement de 3.599 +/- 0.02 et 3.587 +/- 0.02. Cette nouvelle architecture qui offre des possibilités de régénération plus larges tend à garantir au mieux la réussite de la mission mais nécessite la mise en oeuvre d'un élément constitutif supplémentaire.

5.5.5 Discussion

Les résultats obtenus par le biais des simulations nous permettent de mettre en évidence le comportement de l'architecture en mission opérationnelle sur la base du comportement spécifié par les modèles et, notamment, les règles d'agrégation. En ce sens, les simulations mettent en avant des tendances (à ce stade du travail), plutôt que

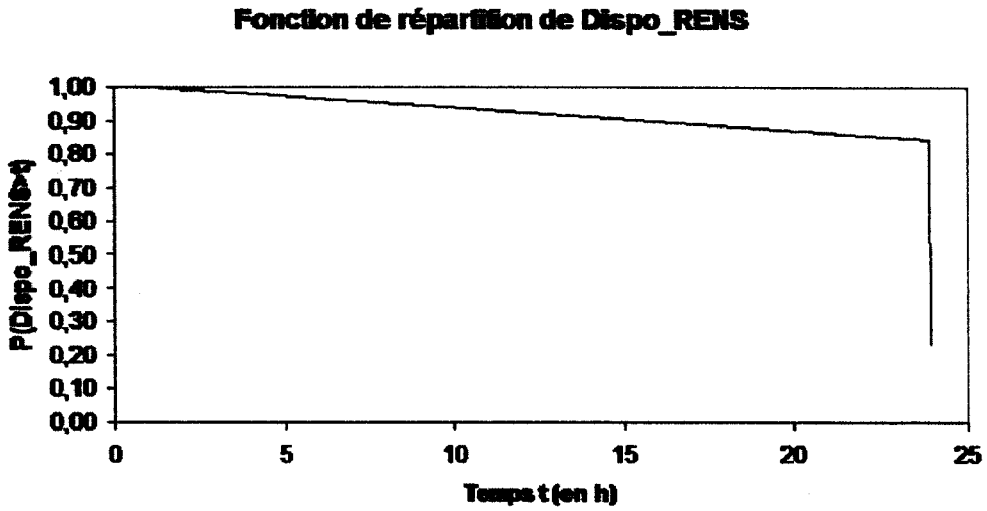

FIG. 5.17 – Fonction de répartition de la variable Dispo_RENS en présence d'une agression et de régénération : reconfiguration par le drone

de permettre une critique fine sur les valeurs numériques obtenues. Nous avons donc mis en évidence :

1. l'effet des agressions sur la disponibilité opérationnelle par rapport à une approche SdF classique,
2. l'apport de la régénération et, plus particulièrement, de la reconfiguration sur les probabilités de réussite de mission.
3. l'impact de la reconfiguration sur d'autres caractéristiques des systèmes, notamment la fiabilité.
4. l'impact des solutions d'architecture sur la régénérabilité et la disponibilité.
5. d'un point de vue plus global, l'applicabilité de la méthodologie proposée.

Nous avons également montré la cohérence des résultats obtenus par simulation avec les résultats obtenus par calcul pour la partie fiabilité du modèle, apportant ainsi les premiers éléments de validation à la modélisation.

5.6 Conclusion

La modélisation et l'évaluation d'une architecture de SdS dérivée d'une architecture de SGTIA a permis de montrer la faisabilité de la méthodologie support de l'ingénierie de régénération proposée. La première phase de la méthodologie nous a donc conduit à définir les tables de données construites sur la base des diagrammes de classe définis

au chapitre III. L'ensemble de ces tables constitue donc le modèle de données dans lequel les informations relatives à l'architecture et à sa mission sont structurées selon les axes définissant le modèle structurel. Nous avons ensuite montré comment ces données peuvent être exploitées par les mécanismes de construction pour définir les atomes de modélisation des constituants et des fonctions à la base du modèle dynamique support des simulations. Relativement à l'architecture de base retenue, deux scénarios de régénération ont été développés et mis en oeuvre dans les simulations. Les résultats obtenus nous ont permis de conclure quant à l'impact de la régénération sur la disponibilité opérationnelle de l'architecture et de valider partiellement la modélisation.

A travers ces premières simulations, nous avons donc mis en évidence les capacités de la méthodologie à fournir un outil d'aide à la décision en conception et en exploitation à travers l'évaluation de solutions de conception (choix de constituants sur des critères : fiabilité, vulnérabilité, coût) et l'évaluation d'architecture opérationnelle pour une mission donnée (choix du nombre et du rôle des plates-formes sur la base de compromis du type régénérabilité/coût) au regard de la disponibilité opérationnelle. Par ailleurs, la construction du cas d'application nous a également permis de mettre en évidence la capacité du modèle structurel à formaliser l'ensemble de la connaissance nécessaire à la construction du modèle dynamique support des simulations pour l'évaluation de la disponibilité opérationnelle dans les différentes configurations de l'architecture retenue.

Conclusion et Perspectives

Conclusion

Dans cette thèse, nous montrons l'intérêt de développer une ingénierie de régénération parfaitement intégrée à l'ingénierie système dans le cadre de l'évaluation des systèmes au regard des exigences de sûreté de fonctionnement et, plus particulièrement, des exigences de disponibilité opérationnelle en mission de combat. Nous proposons donc en ce sens une méthodologie de modélisation des systèmes, support des évaluations de la disponibilité opérationnelle comme premier élément constitutif d'une ingénierie de régénération. En effet, l'évolution des contextes opérationnels et, notamment, des menaces ajoutée aux évolutions des nouvelles technologies de l'information et de la communication offrent des nouvelles perspectives pour les capacités opérationnelles des matériels. Cela a conduit la DGA à repenser le cadre d'emploi des matériels et à définir le concept de Bulle Opérationnelle Aéroterrestre (BOA) dans lequel la définition des systèmes se fait selon un processus d'ingénierie système de systèmes. Ainsi, la mise en réseau de plates-formes au sein d'une architecture donne une nouvelle dimension à la disponibilité opérationnelle notamment en raison des capacités nouvelles attendues de telles architectures. La régénération des matériels au combat qui contribue largement à l'optimisation de la disponibilité opérationnelle constitue une des principales illustrations de ces nouvelles capacités.

Nos travaux sur la modélisation de la disponibilité opérationnelle en présence de défaillances, de dommages et de régénération se justifient par le manque de méthodes et d'outils permettant l'évaluation conjointe des effets des défaillances, des dommages et de la régénération sur la disponibilité opérationnelle d'architecture de système de systèmes. Pour arriver à cette conclusion, nous avons, dans un premier temps, abordé séparément les travaux de modélisation et d'évaluation de la disponibilité (relatifs aux défaillances et à la maintenance), les travaux de modélisation et d'évaluation de la survivabilité (relatifs aux facteurs extérieurs et notamment aux agressions) afin d'identifier quels pouvaient être les points communs et recoupements entre ces différentes approches. Il est donc apparu clairement qu'aucune approche ne permettait (en l'état) de modéliser à la fois les défaillances, les dommages et leur régénération de manière unifiée afin d'obtenir une

évaluation globale de la disponibilité. Dans la plupart des approches rencontrées dans les différentes communautés scientifiques concernées, un des trois aspects fait toujours défaut.

Afin de tirer parti des éléments les plus pertinents pour chacun des aspects (défaillance, dommage et régénération), nous avons proposé une méthodologie de modélisation qui s'appuie sur une modélisation unifiée des défaillances et des dommages et de la régénération. L'intérêt de l'approche unifiée réside dans le fait de pouvoir capturer au sein d'un même modèle le comportement des composants d'un systèmes en présence de défaillances, de dommages et de régénération. La méthodologie repose sur trois étapes :

- formalisation des connaissances nécessaires à la construction du modèle dynamique (étape concrétisée par un modèle structurel statique),
- élaboration du modèle dynamique comportemental (basé sur une représentation des processus stochastiques à l'origine du comportement des systèmes dans le formalisme des Stochastic Activity Networks),
- simulation du modèle dynamique par le biais de simulation Monte Carlo pour l'évaluation des performances des systèmes.

Pour garantir l'intégration de l'ingénierie de régénération à l'ingénierie système, la méthodologie est construite dans le respect de concepts, de méthodes et d'outils issus de travaux scientifiques et reconnus en ingénierie système. Elle intègre également des mécanismes de construction génériques du modèle dynamique qui garantissent au moins partiellement la cohérence entre le modèle statique et le modèle dynamique.
Une architecture représentative de la problématique dérivée d'une architecture concrète de système de systèmes a constitué le support à la mise en oeuvre de la méthodologie de modélisation, nous permettant ainsi d'en démontrer la faisabilité. Les connaissances indispensables à la construction des modèles nous ont été partiellement apportées par la DGA et NEXTER systems en fonction de leurs domaines de compétences respectifs. En effet, la définition des règles d'agrégation qui permettent de déterminer l'état des fonctions en fonction de l'états des constituants qui la supportent constitue une étape délicate qui peut être une source d'erreur. Leur expertise a également constitué une source de validation de l'approche proposée. Des simulations ont finalement pu être réalisées démontrant ainsi l'applicabilité de l'approche et validant les différents comportements attendus pour l'architecture considérée.

Finalement, l'approche proposée constitue la base au développement d'un outil logiciel support de l'ensemble de la méthodologie pour l'évaluation d'architecture au regard de la problématique de la régénération des systèmes. Ainsi, pour NEXTER Systems, un tel outil permettra l'évaluation de solutions de conception des plate-formes relativement à des paramètres de fiabilité, de vulnérabilité et de régénérabilité qui caractérisent les différents constituants et sous-systèmes. Par ailleurs, relativement aux activités de la DGA, un outil intégré support de la méthodologie offrira la possibilité d'évaluer des architectures en fonction du contexte opérationnel dans lequel elles sont mises en oeuvre.

Perspectives

La première perspective à court terme de ces travaux concerne une validation plus poussée de la méthodologie sur une architecture concrète non restreinte sur la taille du système de systèmes afin de valider les principes de modélisation à grande échelle. Il faudra notamment s'assurer que, sur de telles architectures, le modèle structurel tel qu'il est défini n'induit pas de limitations dans la formalisation des connaissances nécessaires à la construction des modèles dynamiques. Cette étape permettra également d'éprouver le formalisme des SANs et leur possibilité de traiter des grands modèles.
Une seconde perspective, toujours dans un objectif de validation, mais à moyen terme concerne la validation des résultats de simulations sur la base d'une modélisation issue d'un retour d'expérience afin de valider les résultats obtenus par les simulation avec des résultats obtenus sur le terrain. Ce type de démarche a notamment déjà été réalisé par la DGA pour des modèles de disponibilité uniquement basés sur la représentation des défaillances et de la maintenance des matériels (DGA 1995). La représentation du comportement proposée dans la méthodologie serait ainsi validée de manière non-ambiguë. Toujours dans une perspective de validation de la faisabilité, la méthodologie doit être mise en oeuvre sur d'autres domaines applicatifs afin d'en valider la généricité.

Une fois les principes à la base de la méthodologie validés, une autre perspective concerne quant à elle l'outil support de la méthodologie. Pour fournir une solution logicielle intégrée implémentable dans les ateliers d'ingénierie système, il est nécessaire de faire porter par un seul outil les différentes phases de la méthodologie. Cet outil devra permettre la génération de bases de données dans le respect du modèle structurel pour intégrer la connaissance liée à des architectures particulières relatives à des missions particulières. Les mécanismes de construction du modèle dynamique devront être complétés afin de pouvoir automatiquement extraire de la base de données les connaissances nécessaires à la construction du modèle dynamique et les reformater dans le formalisme adaptées aux simulations. Un module de traitement des statistiques de simulation devra également être développé afin de rendre lisibles les résultats des simulations.

Toujours à moyen terme, une perspective de recherche consisterait à définir des règles de vérification des règles d'agrégation de manière à garantir un comportement correct des différents sous-modèles évitant notamment la présence de boucles, source d'erreurs dans les simulations. En ce sens, les SANs offrent une plus grande flexibilité de modélisation que les réseaux de Petri mais cette flexibilité se paie par la perte des possibilités des vérification des modèles. Il serait donc également particulièrement intéressant, toujours dans une optique de valider le formalisme retenu, de construire le modèle dynamique suivant le formalisme des réseaux de Petri stochastiques, qui partagent beaucoup d'avantages avec les SANs. Cette étape de validation sera facilitée par les mécanismes de construction proposés, qui ont été définis indépendamment du formalisme support des modèles dynamiques. Il serait donc particulièrement intéressant de travailler à la vérification des modèles.

Une seconde perspective de recherche relativement à la méthodologie proposée consisterait quant à elle en la définition d'indicateurs de régénérabilité des systèmes basés sur la représentation du comportement des systèmes. Une évaluation dynamique des indi-

cateurs de régénérabilité constituerait un outil d'aide à la décision en mission pour les fonctions de commandement particulièrement pertinent pour évaluer dynamiquement *l'aptitude restante* d'un système à être remis en service pour terminer la mission.

Une troisième perspective de recherche relativement à la modélisation d'architecture de système de systèmes revient à la modélisation des fonctions de commandement au sein de l'architecture. Volontairement écartées dans une première approche dans la réalisation de nos travaux, les fonctions de commandement sont primordiales à la réalisation d'une mission. Particulièrement complexes, les architectures de commandement reposent sur des relations complexes entre les plates-formes difficilement représentables avec le formalisme actuel des règles d'agrégation. Des travaux doivent donc être menés plus avant pour :

- identifier les verrous liés à la modélisation des fonctions de commandement,
- proposer des solutions adaptées facilement intégrables à l'ingénierie de régénération.

Liste des publications

M. Monnin and O. Senechal and B. Iung and P. Lelan and M. Garrivet (2006). « A Unified Failure/Damage Approach to Battle Damage Regeneration : Application to Ground Military Systems », *Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2006*, pp. 379 - 384, Beijing, P R. CHINA.

E. Thomas and E. Levrat and B. Iung and M. Monnin (2006). « 'Odds algorithm' - based opportunity - triggered preventive maintenance with production policy », *Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2006*, pp. 835 - 840, Beijing, P R. CHINA.

M. Monnin and B. Iung and O. Sénéchal (2007). « Méthodologie pour l'évaluation de la disponibilité opérationnelle des systèmes d'armes en présence de défaillance, de dommage et de régénération », dans GDR MACS (éd.), *2èmes Journées Doctorales / Journées Nationales MACS, JD-JN-MACS*, Reims, France, CDROM.

M. Monnin and O. Senechal and B. Iung (2007). « A methodology for weapon system availability assessment, incorporating failure, damage and regeneration », *Proceedings of the first IFAC Workshop on Dependable Control of Discrete Systems, DCDS'07*, IFAC, Cachan, FRANCE.

M. Monnin and B. Iung and O. Senechal and P. Lelan (2008). « Dynamic model for assessing impact of regeneration actions on system availability : Application to weapon systems », *Proceedings of the 54th Annual Reliability & Maintainability Symposium (RAMS)*, to be published, Las Vegas, USA.

Bibliographie

AFNOR (2001). « Terminologie de la maintenance », *Normes*, AFNOR.

ALVAREZ, O. E. et POSSAMAI, A. (2002). « Model of Analysis of Project Characteristics for Maintainability – Determining an Index of Maintainability in a Product System Project », *Brazilian Journal of Management of Product Development*, **2**(2).

BALL, R.E. (1985). *The Fundamentals of Aircraft Combat Survivability Analysis and Design*, American Institute of Aeronautics and Astronautics New York, NY.

BARRACO, L. (2006). « La bulle opérationnelle aéroterrestre », *La jaune et la rouge*, pp. 19–24.

BEAUDET, S.T. , COURTNEY, T. et SANDERS, W. H. (2006). « A Behavior-based Process for Evaluatingh Availability Achievement Risk using Stochastic Activity Networks », *Proc. of the 52nd Annual Reliability and Maintainability Symposium (RAMS2006)*.

BETOUS-ALMEIDA, C. (2002). *Construction et affinement de modèles de sûreté de fonctionnement - Application aux systèmes de contrôle-commande*, PhD thesis, LAAS/CNRS, Institut National Polytechnique de Toulouse.

BETOUS-ALMEIDA, C. et KANOUN, K. (2004a). « Construction and Stepwise refinement of dependability models », *Performance Evaluation*, **56** : 277–306.

BETOUS-ALMEIDA, C. et KANOUN, K. (2004b). « Dependability modelling of instrumentation and control systems A comparison of competiting architectures », *Safety Science*, **42**(5) : 457–480.

BLANCHO, P. et DURAND, J. (1999). *Sûreté de fonctionnement et maîtrise des risques. La Maintenabilité*, Centre Technique des Industries Mécaniques (CETIM).

BOBBIO, A. et TRIVEDI, KS (1986). « An aggregation technique for the transient analysis of stiff Markov chaine », *IEEE Transactions on Computers*, **35**(9) : 803–814.

BOITEAU, M. , DUTUIT, Y. , RAUZY, A. et SIGNORET, J.P. (2006). « The AltaRica data-flow language in use : modeling of production availability of a multi-state system », *Reliability Engineering and System Safety*, **91**(7) : 747–755.

CAMPBELL, C. B. et STARBUCK, D. W. (2005). « Methodology for Predicting Recoverability », *ASNE Reconfiguration and Survivability Symposium 2005 (RS 2005)*, Amercian Society Naval Engineers, Jacksonville/Mayport Area.

CHABOT, J.L. , DUTUIT, Y. et RAUZY, A. (2001). « De l'usage de la simulation de Monté Carlo couplée aux réseaux de Petri en Sûreté de Fonctionnement », *3e Conférence Francophone de MOdélisarotion et SIMulation - MOSIM'03 - "Concpetion, Analyse et Gestion des Systèmes Industriels"*, Troyes - France.

CIARDO, G. , MUPPALA, J.K. et TRIVEDI, K.S. (1992). « Analyzing concurrent and fault-tolerant software using stochastic reward nets », *Journal of Parallel and Distributed Computing*, **15** : 255–269.

CLARK, G. , COURTNEY, T. , DALY, D. , DEAVOURS, D. , DERISAVI, S. , DOYLE, J. M. , SANDERS, W. H. et WEBSTER, P. (2001). « The Möbius Modeling Tool », *Proceedings of the 9th International Workshop on Petri Nets and Performance Models*, Aachen, Germany, pp. 241–250.

COUR DES COMPTES (2004). « Le maintien en condition opérationnelle des matériels des armées », *Technical report*, Cour des comptes.

DALY, D. , DEAVOURS, D. D. , DOYLE, J. M. , WEBSTER, P. G. et SANDERS, W. H. (2000). « Möbius : An Extensible Tool for Performance and Dependability Modeling », dans B. R. HAVERKORT, H. C. BOHNENKAMP et C. U. SMITH (éds), *Computer Performance Evaluation : Modelling Techniques and Tools : Proceedings of the 11th International Conference, TOOLS 2000*, number No. 1786 in *Lecture Notes in Computer Science*, Berlin : Springer, Schaumburg, IL, pp. 332–336.

DGA (1995). « Validation du modèle EOLE à partir de données recueillies par le 4e Régiment de Dragons au cours de son engagement dans le Golfe », *Diffusion restreinte*, Délégation Générale pour l'Armement, Centre d'Analyse de Défense.

DGA (2002). « Projet BOA (Bulle Opérationnelle Aéroterrestre) », *Dossier de presse*, Délégation Générale pour l'Armement.

DGA (2005). « Programme d'études amonts "Ingénierie, système de systèmes, de la bulle opérationnelle aéroterrestre, démonstration de technologies clés et développement du battlelab du combat aéroterrestre" », *Diffusion restreinte*, Délégation Générale pour l'Armement.

DIMESH KUMAR, U. , CROCKER, J. , KNEZEVIC, J. et EL-HARAM, M. (2000). *Reliability, Maintenance and Logistic Support - A life Cycle Approach*, Kluwer Academic Publishers.

DOD (1980). « Procedures for performing a failure mode, effects and criticality analysis », *Standard MIL-STD-1629A*, Department of Defense, Washington, DC.

DOD (1992). « Logistic support Analysis », *MIL-STD 1388-1A/2A*, Department of Defense.

DUTUIT, Y. , CHATELET, E. , SIGNORET, J-P. et THOMAS, P. (1997). « Dependability modeling and evaluation by using stochastic Petri Nets : application to two cases. », *Reliability Engineering and System Safety*, **55**(2) : 117–124.

EMAT (n.d.). « Objectif d'état-major "Système de contact futur" », *Diffusion restreinte*, Etat-Major de l'Armée de Terre.

EREAU, J-F (1997). *Réseau de Petri pour l'étude de la disponibilité opérationnelle des systèmes spatiaux en phase d'avant projet*, PhD thesis, LAAS, Université Paul Sabatier, Toulouse.

FRICKS, Ricardo M. , PULIAFITO, Antonio , TELEK, Mikl&#243 ;s et TRIVEDI, Kishor S. (1998). « Applications of non-Markovian stochastic Petri nets », *SIGMETRICS Perform. Eval. Rev.*, **26**(2) : 15–27.

FRICKS, R.M. et TRIVEDI, K.S. (1997). « Modeling Failure Dependencies in Reliability Analysis Using Stochastic Petri Nets », *Proc. European Simulation Multi-conference (ESM '97)*, Istanbul.

GT MODÉLISATION ET OUTILS (2002). « Modèle de données AFIS, Version 2.0 », *Technical report*, AFIS.

HEIN, A. et GOSWAMI, KK (1996). « Conjoint simulation-a technique for the combined performance anddependability analysis of large-scale computer systems », *Proceedings of IEEE International Computer Performance and Dependability Symposium*, pp. 68–77.

HILL, J. et STEINBERG, B. (2005). « Design Feature For Survivability of High Speed Ships », *ASNE Reconfiguration and Survivability Symposium 2005 (RS 2005)*, American Society Naval Engineers, Jacksonville/Mayport Area.

JAMSHIDI, M. (2005). « Systems of systems Engineering - a Definition », *IEEE SMC 2005, Plenary Paper*, Big Island, Hawaii.

KEROMYTIS, A. D. , PAREKH, J. , GROSS, P. N. , KAIDER, G. , MISRA, V.l , NIEH, J. , RUBENSTEIN, D. et STOLFO, S. (2003). « A Holistic Approach to Service Survivability », *Technical Report CS-TR-739*, Columbia University, Department of Computer Science, Department of Electrical Engineering.

KNIGHT, John G. et SULLIVAN, Kevin J. (2000). « On the Defintion of Survivability », *Technical Report CS-TR-33-00*, University of Virginia, Department of Computer Science.

LABEAU, P.E. et ZIO, E. (2002). « Procedures of Monte Carlo transport simulation for applications in system engineering », *Reliability Engineering and System Safety*, **77**(3) : 217–228.

LAPORTE, H. (2004). « Etude SC^3 - BOA Rapport final Tome 9 », *Diffusion restreinte*, EADS - MBDA.

L'ECUYER, P. (1996). « Maximally Equidistributed Combined Tausworthe Generators », *Mathematics of Computation*, **65**(213) : 203–213.

LEE, D. , LEE, S.S. , PARK, B.J. et KIM, S.Y. (2005). « A study on the framework for survivability assessment system of damaged ships », *Ocean engineering*, **32**(8-9) : 1122–1132.

LEVITIN, G. et LISINANSKI, A. (2000). « Survivability maximization for vulnerable multi-state systems with bridge topology », *Reliability engineering and System Safety*, **70**(2) : 125–140.

LEVITIN, G. et LISNIANSKI, A. (2003). « Optimizing survivability of vulnerable series-parallel multi-state systems », *Reliability engineering and System Safety*, **79**(3) : 329–331.

LEVITIN, G. , DAI, Y. , XIE, M. et POH, K. Leng (2003). « Optimizing survivability of multi-state systems with multi-level protection by multi-processor genetic algorithm », *Reliability Engineering and System Safety*, **82**(1) : 93–104.

LIEW, S. C. et LU, K. W. (1994). « A framework for characterizing disaster-based network survivability », *IEEE Journal on Selected Area in Communication*, **12**(1) : 52–58.

LIU, Y. , B. MENDIRATTA, V. et S. TRIVEDI, Kishor (2004). « Survivability Analysis of Telephone Access Network », *Proceedings of the 15th IEEE Internationnal Symposium on Software Engineering (ISSRE'04)*, Saint Malo, Bretagne, FRANCE.

LIU, Yun et TRIVEDI, Kishor S. (2004). « A General Framework for Network Survivability Quantification », *12th GI/IT Conference an Measuring, Modelling and Evaluation of Computer and Communication Systems*, Dresden, GERMANY.

MACHERET, Y. , KOEHN, P. et SPARROW, D. (2005). « Improving Reliability and Operational Availability of Military Systems », *Aerospace, 2005 IEEE Conference*, pp. 1–11.

MALHOTRA, M. et TRIVEDI, K. S. (1995). « Dependability Modeling Using Petri-Net Based Model », *IEEE Transactions on Reliability*, **38**(3) : 428–440.

MALHOTRA, M. et TRIVEDI, KS (1994). « Power-hierarchy of dependability-model types », *Reliability, IEEE Transactions on*, **43**(3) : 493–502.

MANTHORPE, W.H. (1996). « The Emerging Joint System of Systems : A Systems Engineering Challenge and Opportunity for APL », *John Hoopkins APL Technical Digest*, **17**(3) : 305–310.

MARQUEZ, A.C. , HEGUEDAS, A. S. et IUNG, B. (2005). « Monte Carlo based assessment of system availability. Acase study for cogeneration plants », *Reliability Engineering and System Safety*, **88** : 273–289.

MARSAN, M.A. , BALBO, G. et CONTE, G. (1984). « A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems », *ACM Transactions on Computer Systems*, **2**(2) : 93–122.

MARSEGUERRA, M. , PADOVANI, E. et ZIO, E. (1999). « The impact of the operating environment on the design of redundant configurations », *Reliability Engineering and System Safety*, **63**(2) : 155–160.

MEINADIER, J-P. (2002). *Le metier d'intégration de systèmes*, Hermès - Lavoisier.

MEYER, J.F. , MOVAGHAR, A. et SANDERS, W.H. (1985). « Stochastic Activity Networks : Structure, Behavior, and Application », *International Workshop on Timed Petri Nets table of contents*, pp. 106–115.

MONNIN, M. , IUNG, B. et SÉNÉCHAL, O. (2007a). « Méthodologie pour l'évaluation de la disponibilité opérationnelle des systèmes d'armes en présence de défaillance, de dommage et de régénération », dans GDR MACS (éd.), *2èmes Journées Doctorales / Journées Nationales MACS, JD-JN-MACS*, Reims, France, p. CDROM.

MONNIN, M. , IUNG, B. , SENECHAL, O. et LELAN, P. (2008). « Dynamic model for assessing impact of regeneration actions on system availability : Application to weapon systems », *Proceedings of the 54th Annual Reliability & Maintainability Symposium (RAMS)*, to be published, Las Vegas, USA.

MONNIN, M. , SENECHAL, O. et IUNG, B. (2007b). « A methodology for weapon system availability assessment, incorporating failure, damage and regeneration », *Proceedings of the first IFAC Workshop on Dependable Control of Discrete Systems, DCDS'07*, IFAC, Cachan, FRANCE.

MONNIN, M. , SENECHAL, O. , IUNG, B. , LELAN, P. et GARRIVET, M. (2006). « A Unified Failure/Damage Approach to Battle Damage Regeneration : Application to Ground Military Systems », *Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2006*, to be published, Beijing, P R. CHINA.

MORTUREUX, Yves (2001). « La sûreté de fonctionnement : méthodes pour maîtriser les risques », *Techniques de l'Ingénieur,,* .

MOVAGHAR, A. (n.d.). « Stochastic Activity Networks : A New Definition », *Proc. of the IASTED Int. Conf. on Modeling and Simulation (MS'97)*, pp. 27–30.

MULLER, A. (2005). *Contribution à la maintenance prévisionnelle des systèmes de production par la formalisation d'un processus de pronostic*, PhD thesis, Université Henri Poincaré, Nancy.

MUPPALA, J. , FRICKS, R. et TRIVEDI, K. S. (2000). *Computational Probability*, Kluwer Academic Publishers, chapter Techniques for System Dependability Evaluation, pp. 445–480.

MUPPALA, J. K. et TRIVEDI, K. S. (1995). « System Dependencies in Markov Dependability Modelling », *Fault-Tolerant System and Software Proceedings of FTS-95*, Narosa Publishing House, New Deli, INDIA, pp. 38–47.

NATO (1994). « STANAG 2418 BATTLE DAMAGE REPAIR POLICY », *Technical report*, NATO.

OMG (2003). « UML, The Unified Modelling Language specifications 1.5 », *Technical report*, OMG.

PAL, P. P. , LOYALL, J. P. , SCHANTZ, R. e. et ZINKY, J.A. (2000). « Open Implementation Toolkit for Building Survivable Application », *DARPA Information Survivability Conference and Exposition Proceedings*, Vol. 2, pp. 197–210.

PAPANIKOLAOU, A. et BOULOUGOURIS, A. (1998). « Design Aspetcs of Survivability of Surface Naval and Merchant Ships », *Proceedings of the 4th Workshop on Ship Stability*, Memorial Univ. of Newfoundland, St. John's, CANANDA.

PEI, R. S. (2000). « Systems of Systems Integration (SoSI) - A smart way of acquiring Army C4I2WS Systems », *Proceeding of the Summer Computer Simulation Conference*, pp. 574–579.

PERRIN, J. , ESTEVE, P. et LE VERN, X. (2001a). « La régénération, de la conception à l'exploitation des systèmes », *DGA : Délégation Générale pour l'Armement,* .

PERRIN, J. , ESTEVE, P. et LE VERN, X. (2001b). « Régénération des matériels au combat », *Etude prospective technico-operationnelle, **DIFFUSION RETSREINTE***, DGA : Délégation Générale pour l'Armement.

RAJE, D.V. , OLANIYA, R.S. , WAKHARE, P.D. et DESHPANDE, A.W. (2000). « Availability assessment of a two-unit stand-by pumping system », *Reliability Engineering and System Safety*, **68**(3) : 269–274.

REGULATION, Army (2005). « Integrated Logistics Support », *Technical Report 700-127*, Headquarters Department of the Army.

REIBMAN, A. et TRIVEDI, K. (1988). « Numerical transient analysis of Markov models », *Computers and Operations Research*, **15**(1) : 19–36.

RESS (1991). « Dependent failure analysis - Special Issue », *Reliability Engineering and System Safety*, **34**(3).

REVILLA, Arturo , CHRISTIANSON, Nora , GUNDERSON, Eric , OCHOA, Cruz , zum BRUNNEN, Rick et MCDONALD, Thomas (2003). « Information Operations Vulnerability/Survivability Assessment (IOVSA) : Procsess Structure (Revision A) », *Technical Report ARL-TR-2993*, Army Research Laboratory.

ROSAIN, N. et LE VERN, X. (2004). « Etude d'architecture du système de cohérence du combat de contact (SC^3) et de la mise en place de la Bulle Opérationnelle Aeroterrestre (BOA) », *Diffusion restreinte*, Thales - Giat Industries.

SAGE, A.P. et CUPPAN, C.D. (2001). « On the Systems Engineering and Management of Systems of Systems and Federations of Systems », *Information, Knowledge, Systems Management*, **2**(4) : 325–345.

SALVILA, C-A. (2005). « Fuzzy Approach for Maintainability Evaluation in the Design Process », *Concurrent Engineering*, **13**(4) : 291–300.

SANDERS, W. H. (1988). *Construction and Solution of Performability models based on Stochastic Activity Networks*, PhD thesis, University of Michigan.

SANDERS, W.H. et MEYER, J.F. (1986). « METASAN :A performability Evaluation Tool Based on Stochastic Activity Networks », *Proceedings of the IEEE-ACM Fall Joint Computer Conference*, Dallas, TX, pp. 807 – 816.

SANDERS, W.H. et MEYER, J.F. (2001). « Stochastic Activity Networks : Formal Definitions and Concepts », *Lecture Notes in Computer Science*, **2090** : 315.

SANDERS, W.H. , OBAL II, W.D , QURESHI, A. et WIDJANARKO, F.K. (1995). « The *Ultra*SAN Modeling Environment », *Perfirmance Evaluation*, **24**(1) : 89 – 115.

SANTOS, T.A. et SOARES, C.G. (2005). « Monte Carlo simulation of damaged ship survivability », *Proceedings of the Institution of Mechanical Engineers, Part M : Journal of Engineering for the Maritime Environment*, **219**(1) : 25–35.

SÉNÉCHAL, O. (2004). *Pilotage des systèmes de production vers la performance globale*, Habilitation à diriger des recherches, Université de Valenciennes et du Hainaut Cambresis (UVHC).

STILLMAN, A. J. (1999). *« Model Composition Within the Möbius Modeling Framework »*, Master's thesis, University of Illinois.

TARELKO, W. (1995). « Control model of maintainability level », *Reliability Engineering & System Safety*, **47**(2).

TARVAINEN, P. (2004). « Survey of the Survivability of IT Systems », *Proceedings of the Ninth Nordic Workshop on Secure IT Systems*, Helsinki, University of Technology, pp. 15–20.

TOGUYÉNI, A. , BERRUET, P. et CRAYE, E. (2003). « Models and Algorithms for Failure Diagnosis and Recovery in FMSs », *The International Journal of Flexible Manufacturing Systems*, **15** : 57–85.

TOMALA, F. (2002). *Proposition of models and methods for performance evaluation-aid of an innovation from its conception*, PhD thesis, (in French), University of Valenciennes and Hainaut Cambrésis (UVHC), Valenciennes, FRANCE.

TRIVEDI, K. S. , VASIREDDY, R. , TRINDADE, D. , NATHAN, S. et CASTRO, Rick (2006). « Modeling High Availability Systems », *Pacific Rim Dependability Conference, PRDC.*

TRIVEDI, K.S. et MALHOTRA, M. (1993). « Reliability and Performability Techniques and Tools : A Survey (Invited Paper) », *Proc. 7th ITG/GI Conference on Measurement, Modelling and Evaluation of Computer and Communication Systems, Aachen University of Technology*, pp. 27–48.

UPADHYA, K. S. et SRINIVASAN, N. K. (2003). « Availability of Weapon Systems with Logistic Delays : A Simulation Approach », *International Journal of Quality and Reliability Management*, **10**(4) : 429–443.

UPADHYA, K. S. et SRINIVASAN, N. K. (2004). « Availability of Weapon Systems with Air-attack Missions », *JDMS : The Journal of Defense Modeling and Simulation : Applications, Methodology, Technology*, **1**(2) : 111–121.

UPADHYA, K. S. et SRINIVASAN, N. K. (2005). « System Simulation for Availability of Weapon Systems under Various Missions », *Systems Engineering*, **8**(4) : 309–322.

WANG, H. et PHAM, H. (1997). « Survey of reliability and availability evaluation of complex networks using Monte Carlo Techniques », *Micoelectron. Reliab.*, **37**(2) : 187–209.

WANI, M.F. et GANDHI, O.P. (1999). « Development of maintainability index for mechanical systems », *Reliability & System Safety*, **65**(3) : 259–270.

WILLIAMSON, A. L. (1998). *« Discrete Event Simulation in the Möbius Modeling Framework »*, Master's thesis, University of Illinois.

ZIO, E. , PODOFILLINI, L. et ZILLE, V. (2006). « A combination of Monte Carlo simulation and cellular automata for computing the availability of complex network systems », *Reliability Engineering and System Safety*, **91**(2) : 181–190.

ZWINGELSTEIN, G. (1995). *Diagnostic des défaillances*, Hermès, Paris.

ZWINGMANN, X. (2005). *Modèle d'évaluation de la fiabilité et de la maintenabilité au stade de la conception*, PhD thesis, Faculté des études supérieures de l'Université Laval, Québec.

TITRE : Approche unifiée défaillance/dommage pour la régénération des matériels au combat : Application aux systèmes d'armes terrestres

Résumé : La Délégation Générale pour l'Armement (DGA) participe à la définition du concept de Bulle Opérationnelle Aéroterrestre (BOA), dans laquelle les systèmes doivent intégrer des possibilités de régénération afin de garantir l'accomplissement de la mission. Aussi, NEXTER Group qui conçoit et développe les systèmes d'armes répondant aux besoins des armées se doit de garantir la disponibilité opérationnelle des systèmes livrés en y intégrant les actions de régénération possibles. Cela nécessite de pouvoir disposer dès les phases de conception de modèles supports à l'évaluation de la disponibilité intégrant l'impact des défaillances, des dommages et de la régénération. Cependant, si défaillance et dommage constituent des éléments maîtrisés dans la conception des systèmes d'armes au travers des études de sûreté de fonctionnement d'une part et de survivabilité d'autre part, la prise en compte de la régénération souffre du manque de méthodes et d'outils de modélisation permettant de considérer conjointement défaillance et dommage. En ce sens, notre contribution porte sur une démarche méthodologique de modélisation basée sur les principes de représentation des systèmes empruntés à l'ingénierie système, et sur une représentation unifiée défaillance/dommage. La méthodologie permet la construction d'atomes génériques de modélisation des constituants et des fonctions représentatifs du comportement des systèmes. Ces atomes permettent la construction d'un modèle dynamique basé sur le formalisme des Stochastiques Activity Networks, support des évaluations. La mise en œuvre de la méthodologie sur une architecture de système de systèmes définie par la DGA et Nexter démontre la faisabilité de la méthodologie proposée aussi bien d'un point de vue de la définition de solutions de conception que d'un point de vue d'évaluation d'architectures opérationnelles relativement à un profil d'emploi.

Mots-clés : Défaillance, Dommage, Régénération, Sureté de fonctionnement, Survivabilité, Ingénierie Système, Stochastic Activity Networks, Simulations.

TITLE : Unified failure/damage approach for system regeneration : Application to ground military systems

Abstract : The French Procurement Agency (DGA) aims at defining the needs of French Army and actually work to define the BOA (airland operational bubble). In this particular operational context military systems have to integrate regeneration facilities defined has system's ability to return damaged or disabled component to temporary service in order to fulfil its mission. Nexter group which designs and manufactures armoured vehicles to meet the needs of Army has to guarantee the operational availability of the systems they sell. Thus, operational availability assessment has to integrate failure damage and regeneration in the same modelling process. Although failure are considered in dependability framework and damage are studied in the survivability framework, taking into account regeneration remains difficult due to the lack of modelling methods and tools that incorporate failure damage and regeneration in a unified way. In that way, our contribution is related to a modelling method based on system engineering that allows defining a generic modelling atom for the system behaviour representation. A dynamic model based on the modelling atoms aggregation has been developed by means of Stochastic Activity Networks that allow simulations to be completed for the availability assessment. The feasibility and the added value of the approach is experimented on a system architecture jointly defined by the DGA and Nexter Group.

Keywords : Failure, Damage, Regeneration ; Dependability, Survivability, System Engineering, Stochastic Activity Networks, Simulations.