Méthodologie pour l'évaluation de la disponibilité opérationnelle des systèmes d'armes en présence de défaillance, de dommage et de régénération

Maxime Monnin, Benoît Iung, Olivier Sénéchal

Méthodologie pour l'évaluation de la disponibilité opérationnelle des systèmes d'armes en présence de défaillance, de dommage et de régénération

Maxime Monnin[1], Benoît Iung[2],Olivier Sénéchal[1],

[1]LAMIH UMR CNRS 8530
Université de Valenciennes, Le Mont Houy, 59313 Valenciennes Cedex 9, France

maxime.monnin@cran.uhp-nancy.fr, olivier.senechal@univ-valenciennes.fr

[2]CRAN UMR CNRS 7039
Nancy Université, Faculté des Sciences, BP 239, 54506 Vandoeuvre-lès-Nancy, France

benoit.iung@cran.uhp-nancy.fr

Résumé

La disponibilité opérationnelle est un facteur déterminant dans la caractérisation des systèmes. Évoluant dans un contexte hostile, les systèmes d'armes sont eux particulièrement vulnérables en cas d'indisponibilité survenant sur un théâtre d'opérations. La disponibilité opérationnelle des systèmes d'armes peut être affectée par des défaillances mais également par les dommages relatifs aux agressions à l'encontre du système et dans les deux cas la régénération du système est primordiale. Cependant, peu d'études considèrent les dommages et la régénération dans l'évaluation de la disponibilité opérationnelle. Sur la base d'une approche unifiée défaillance/dommage et des techniques de modélisation états-transitions, ce papier définit les principes méthodologiques d'une modélisation des systèmes intégrant les défaillances, les dommages et la régénération pour l'évaluation de la disponibilité en mission opérationnelle. La modélisation est supportée par le formalisme des Stochastic Activity Networks.

Mots-clés

Dommages, défaillances, régénération, évaluation de la disponibilité, Stochastic Activity Networks, simulation de Monte Carlo.

I. Introduction

De plus en plus, la disponibilité opérationnelle constitue une performance clé des systèmes, plaçant ainsi la Sûreté de Fonctionnement (SdF) au coeur des préoccupations dans la définition des systèmes. Beaucoup de systèmes critiques au regard de leur mission (e.g. systèmes d'information, réseaux informatiques) sont amenés à être exploités dans des conditions hostiles [1]. La disponibilité opérationnelle de tels systèmes n'est donc plus majoritairement affectée par les défaillances mais dépend également de facteurs extérieurs. Ceci est d'autant plus vrai pour les systèmes d'armes, conçus pour évoluer en mission de combat [2]. La fiabilité et la vulnérabilité et plus largement la SdF et la survivabilité sont donc deux caractéristiques primordiales de ces systèmes. En effet, de ces deux propriétés va notamment dépendre la survie de l'équipage et la réussite de la mission. Ainsi, l'aptitude du système à recouvrer des capacités opérationnelles en mission de combat après l'occurrence d'une défaillance ou d'un dommage par des actions de régénération apparaît comme une nouvelle exigence dans la définition des systèmes [3]. La considération nécessite donc de prendre en compte l'impact des défaillances d'une part et des dommages d'autre part.

Dans le contexte des études de SdF, la disponibilité dépend de la fiabilité et de la maintenabilité. La plupart des travaux actuels sont basés sur une approche probabiliste de la SdF décrivant le comportement des systèmes avec des méthodes de type états-transitions permettant de représenter des comportements complexes [4]. Les approches typiques de modélisation de la disponibilité reposent sur l'utilisation des chaînes de Markov et des réseaux de Petri. De nombreux modèles ont été développés représentant des comportements de type défaillance/réparation et autorisant une évaluation de la disponibilité soit de manière analytique soit par simulation, [4], [5]. Plus récemment, des travaux relatifs à la dynamique de la dégradation, pour l'évaluation des performances de SdF et l'optimisation de la maintenance, ont été introduits [6]. Toutes ces approches sont basées sur la fiabilité et la maintenabilité mais ne considèrent pas de facteurs extérieurs. En SdF, les facteurs extérieurs sont traités relativement au concept de *défaillances de cause commune* [7]. Les différents modèles proposés s'attachent à formaliser des redondances de type k-out-of-n où les éléments sont identiques et où les actions de maintenance ne sont pas prises en compte. Une autre approche relative à la considération des facteurs extérieurs (i.e. les dommages) a été développée par [8]. Les dommages sont considérés comme des événements aléatoires modélisés par une distribution de probabilité discrète pouvant conduire soit à la destruction du système, soit à une défaillance du système. L'impact physique des dommages est donc pris en compte à travers la destruction des systèmes. Cependant, les actions de maintenance considérées nécessitent un arret de la mission pour le système et la maintenabilité est identique en cas de

défaillance ou de défaillance suite à un dommage. Outre la destruction, l'impact physique des dommages tels que définis dans [9] et les conséquences sur les critères de maintenabilité (accessibilité, assemblage/désassemblage,...) ne sont pas modélisés. Parallèlement à la SdF, les études de survivabilité initialement concernée par l'impact des agressions sur les systèmes ont été étendues aux défaillances et la définition suivante tend à se généraliser :*aptitude d'un système à terminer sa mission en présence d'attaques, de défaillances ou d'accidents [1].* Cependant, si l'impact physique des dommages intervient à travers la vulnérabilité des systèmes dans les modèles, aucune action de réparation n'est considérée dans l'évaluation de la survivabilité [2]. D'autres modèles intègrent des actions de réparation/reconfiguration dans un contexte d'évaluation de la survivabilité en s'inspirant des modèles classiques de SdF [10]. Dommage et défaillance conduisent aux mêmes états et correspondent à des événements aléatoires distribués exponentiellement. Le recouvrement de capacités fonctionnelles dans le cadre de la survivabilité est également abordé dans [3]. L'impact physique des dommages est traité dans un contexte militaire mais il n'y pas d'évaluation quantitative de l'impact du possible recouvrement de capacités fonctionnelles sur la disponibilité des systèmes.
Le constat global émergent des contributions précédemment citées, est qu'il n'y a pas dans les modèles actuels de considération de l'impact physique des dommages ainsi que leur régénération dans l'évaluation de la disponibilité opérationnelle. Relativement à ce constat, les travaux présentés dans cet article - financés par la Délégation Générale pour l'Armement (DGA) - trouvent leur genèse dans [11] et ont un champ d'application relatif aux systèmes d'armes avec pour support, les systèmes développés par NEXTER (anciennement Giat Industries) partenaire industriel de la thèse.
Nous proposons dans ce papier une *approche unifiée défaillance/dommage* basée sur le parallèle entre défaillances et dommages établi dans [11] pour la modélisation des systèmes et l'évaluation de la disponibilité opérationnelle en présence de défaillances, de dommages et de régénération. Le modèle dynamique nécessaire à la phase d'évaluation est basé sur les Stochastic Activity Networks (SANs) avec un couplage à des simulations de Monte Carlo. En effet, l'approche unifiée se justifie par le manque de méthodes et d'outils permettant d'évaluer la disponibilité opérationnelle des matériels au combat en considérant d'une part les défaillances inhérentes à tout système technique et d'autre part les dommages liés au contexte opérationnel des systèmes d'armes, tout en intégrant des possibilités de régénération.
La suite de cette communication est organisée de la façon suivante : la section 2 expose un exemple de système de systèmes qui servira de support à la présentation de la démarche de modélisation proposée. Les principes de modélisation seront présentés dans la section 3. Dans la section 4, nous montrons comment les SANs peuvent supporter la modélisation et des résultats de simulations sont présentés sur la base du modèle relatif à l'exemple de la section 2. Enfin, en section 5 une conclusion clôt l'exposé.

II. Exemple support de la démarche : Système de Systèmes (SdS)

Le système retenu pour illustrer la démarche de modélisation et d'évaluation s'inscrit dans le nouveau contexte de définition des systèmes de contact relatif à la Bulle Opérationnelle Aéroterrestre (BOA), [12]. Le système de contact est vu comme un système de systèmes (SdS) défini en terme de capacités opérationnelles globales (liées à sa mission) ; ces performances globales étant déclinées et allouées sur les différentes plates-formes (systèmes d'armes) au sein desquelles les fonctions du système de contact sont réparties. Une vision réduite d'un système de contact est présentée dans cet exemple (figure 1). Le système retenu est défini autour d'une mission de type "Reconnaissance d'un point" face à une menace missile, tiré depuis un blindé lance-missiles antichar. La mission est supposée durer vingt-quatre heures et la probabilité d'occurrence de la menace pour la mission est $P_{occurrence} = 0.8$. Trois plates-formes participent à la fonction Renseignement (RENS) du SdS : deux plates-formes dont la fonction principale est une fonction d'observation (OBS) et une plate-forme dotée d'une capacité de tir (fonction FEU). Les plates-formes d'observation doivent informer la plate-forme de tir sur les positions adverses. Pour chaque système, on suppose que les fonctions principales sont supportées par deux sous-systèmes. Les performances des différentes fonctions (RENS, OBS et FEU) sont spécifiées suivant 4 niveaux : Nominal, Dégradé, Secours et Panne définissant ainsi les états possibles pour les fonctions.

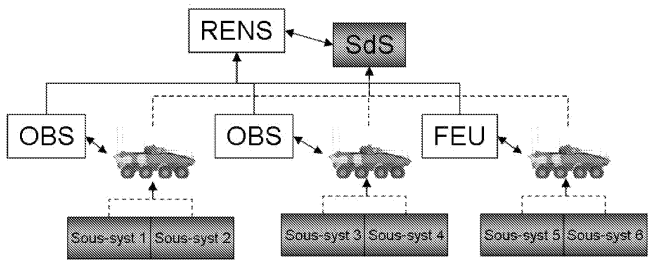

Fig. 1. Exemple d'architecture organico-fonctionnelle de SdS

III. Modélisation des défaillances, des dommages et de la régénération

L'approche proposée pour la modélisation est résumée dans la figure 2, [13] et met en évidence notre contribution scientifique sur quatre point essentiels :

1. la formalisation de la structure du système par un modèle de données : *le modèle structurel*, supporté par le langage UML. Cette première représentation permet de prendre en compte au sein d'un même modèle des aspects relatifs aux défaillances et aux dommages (décomposition organique, fonctionnelle, localisation des composants, données de vulnérabilité, de fiabilité, scénario opérationnel,...),

2. la définition de mécanismes de construction d'un modèle dynamique support des évaluations. Ces mécanismes définissent le passage du modèle structurel (statique) vers le modèle dynamique et en garantissent ainsi la cohérence avec la description du système,

3. la proposition d'un atome générique de représentation du comportement des composants (sous-systèmes) en présence de défaillance, de dommage et de régénération, à la base du modèle dynamique, supporté dans son ensemble par le formalisme des Stochastic Activity Networks (SANs),

4. éprouver le formalisme des SANs, au regard de la problématique abordée :
- mise en évidence de l'exploitabilité à travers la possibilité de supporter l'atome de modélisation et plus largement l'ensemble du modèle dynamique,
- passage à l'échelle dans le cas d'un modèle de système de systèmes (grands nombres d'états dans le modèle, interactions et dépendances nombreuses).

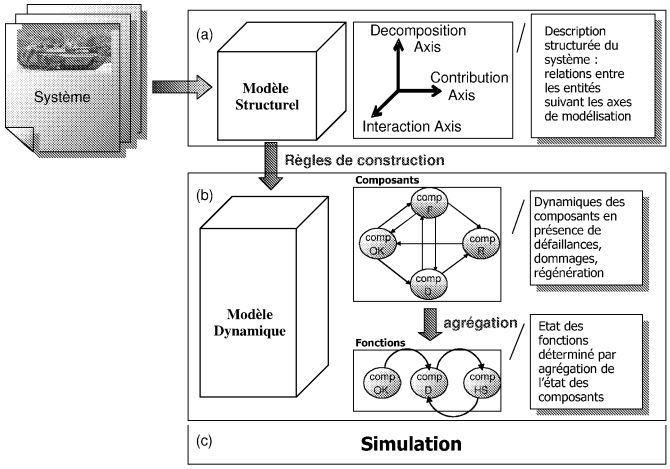

Fig. 2. Approche de modélisation pour la régénération

Les deux premiers points ont déja été abordés dans [13] et ce papier se focalise tout d'abord sur la description de l'atome de modélisation et montre ensuite comment cet atome peut être porté par le formalisme des SANs. Le modèle dynamique SAN correspondant à l'exemple donné à la section II est présenté ainsi que les résultats de 3 scénarii de simulations.

A. Les défaillances

Une défaillance au niveau des sous-systèmes implique la perte de la fonction opérationnelle supportée par les sous-systèmes (impact fonctionnel). Du point de vue de la fiabilité, les sous-systèmes peuvent donc être vus suivant un comportement binaire avec deux états : un état "Ok" et un état "Panne". Le passage de l'état "Ok" à l'état "Panne" peut ainsi être représenté par la fonction de défiabilité des sous-systèmes (la fiabilité étant supposée exponentielle à taux constant λ). Chaque sous-système i sera donc caractérisé par son taux de défaillance λ_i. Une représentation générique du comportement d'un sous-système en présence de défaillance est représenté à la figure 3. Pour poursuivre l'exemple de la section II, les taux de défaillances des sous-systèmes considérés sont donnés dans la table I.

B. Les dommages

Selon la norme [9], les études de dommages se basent sur des modes de dommage génériques (e.g. pénétration, coupé, déformé, explosé,...), relatifs à l'impact physique des agressions sur les composants considérés. Tout en entraînant une perte de la fonction opérationnelle, les dommages vont donc nécessairement modifier la maintenabilité des composants et conditionner les actions de régénération envisageables. Pour prendre en compte l'impact des dommages sur la maintenabilité, outre leur fonction opérationnelle, les composants sont supposés avoir des fonctions techniques relatives aux critères de maintenabilité. Ces fonctions techniques vont donc permettre de rendre compte de la régénérabilité des composants en considérant d'une part la maintenabilité intrinsèque (fonction des dispositions constitutives du système) et d'autre part l'impact physique de dommages. Ainsi, comme la défaillance entraîne la perte de la fonction opérationnelle, les dommages vont affecter les fonctions techniques et conditionner les actions de régénération possibles. Par exemple, un dommage de type "explosion" va affecter le critère d'accessibilité et donc les fonctions techniques de conditionnement et de fixation. La seule régénération possible sera une reconfiguration (faire supporter la fonction opérationnelle perdue

par un autre composant), le composant atteint n'étant plus accessible pour réparation ou échange.
Pour modéliser le comportement des sous-systèmes en présence d'agression (i.e. les dommages qui en résultent), trois types de dommages sont considérés, relativement à la classification des dommages donnée dans [14]. Le premier type de dommage est relatif à la détérioration du materiel (les fonctions techniques sont atteintes). Le deuxième type de dommage est relatif à la destruction du matériel (la fonction opérationnelle est perdue et les fonctions techniques sont atteintes). Enfin, le troisième type concerne les effets indirects des dommages (propagation des dommages) suivant lesquels les fonctions techniques sont intactes mais la fonction opérationnelle est perdue (cf. "Secondary damage effects" dans [9]). Pour considérer ces trois types de dommage il est nécessaire d'introduire de nouveaux états dans le modèle pour prendre en compte dans ce même modèle défaillance et dommage. Aux états "Ok" et "Panne" définis précédemment nous proposons d'ajouter un état "Détérioré" reflétant les conséquences de dommage relatif à la détérioration et un état "Détruit" correspondant à l'état après un dommage relatif à la destruction du matériel. Pour le troisième type de dommage, l'état "Panne" permet de représenter les conséquences d'un dommage relatif à un impact fonctionnel (ou une propagation de dommage). Comme l'état "Panne" intervient après l'occurrence d'une défaillance, les différents états relatifs aux dommages interviennent après l'occurrence d'une agression, et peuvent se propager d'un composant à un autre : des composants proches (en terme de localisation dans le système) peuvent être impactés simultanément et l'endommagement d'un composant peut également soit conduire directement à la défaillance d'un autre, soit accélérer le processus de dégradation (modification du taux de défaillance λ). Trois types d'agressions sont considérées : 1. agression mineure conduisant à l'état "détérioré", 2. agression majeure conduisant à l'état "Détruit" et 3. agression *fonctionnelle* conduisant à l'état "Panne". Ainsi, le comportement des sous-systèmes en présence de défaillance et de dommage peut être représenté par le modèle (conceptuel) donné à la figure 3. Le troisième type d'agression n'est pas considéré dans la suite du papier. Ainsi, une agression sera donc caractérisée par sa probabilité d'occurrence pour la mission considérée, sa probabilité d'atteindre chacun des sous-systèmes et enfin par son type. En effet, une même catégorie d'agression peut prendre différents types et impacter ainsi différemment les sous-systèmes. Les études de vulnérabilité s'attachent donc à définir ces probabilités. En s'appuyant sur les exemples fournis dans [11], on peut définir pour chaque sous-système considéré dans notre exemple (section II) les probabilités d'atteinte ainsi que les probabilités d'occurrence relatives aux agressions mineures et majeures pour une catégorie d'agression considérée (i.e. missile, tiré depuis un blindé lance-missiles antichar). Ces probabilités sont caractérisées par des distributions discrètes à support fini (e.g. pour le type d'agression on considère le support S avec $S = \{Détruit,\ Détérioré\}$). Les probabilités relatives à notre exemple sont données dans la table I, (ces valeurs sont indicatives, les données réelles étant confidentielles).

TABLE I
TAUX DE DÉFAILLANCE ET PROBABILITÉ DE DOMMAGES

Sous-syst.	Agression : Missile			
	λ (en h^{-1})	P_{Atteint}	$P_{\text{Détruit}}$	$P_{\text{Détériore}}$
1	2.0E-5	0.12	0.2	0.8
2	5.0E-4	0.12	1	0
3	5.0E-4	0.12	0.2	0.8
4	2.0E-5	0.52	1	0
5	1.0E-6	0.06	0.2	0.8
6	2.0E-6	0.06	0.2	0.8

C. La régénération

La régénération a pour objectif de redonner aux systèmes des capacités opérationnelles après l'occurrence d'une défaillance ou d'un dommage afin qu'il soit en mesure de poursuivre sa mission. En ce sens, elle participe à la survivabilité (telle que définie dans la section I) dans la mesure où elle va améliorer la disponibilité opérationnelle des systèmes. Comme la Réparation des Dommages subis au Combat (RDC) (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, [15]), la régénération s'effectue en mission et ne dispose pas de tous les moyens mis en oeuvre dans un contexte de maintenance. La régénération peut donc être définie de façon similaire à la RDC en ajoutant la notion de défaillance : *Réparation essentielle, pouvant être improvisée et/ou temporaire, effectuée rapidement dans des conditions de combat, afin de remettre en service le matériel endommagé, immobilisé ou défaillant.* Compte tenu de ses caractéristiques, la régénération peut s'inscrire dans le premier des trois niveaux techniques d'intervention de la fonction maintenance dans les armées, le NTI 1. En effet, suivant ce niveau, 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). Ainsi, trois types d'actions peuvent être considérés pour la régénération : A. la reconfiguration, B. le dépannage, C. l'échange.

A. 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 [16]. Cette définition est donc appliquée dans le cas de défaillance ou de dommage. Elle constitue une action de régénération qui met en œuvre au moins 2

composants : un composant atteint (état "panne", "détérioré" ou "détruit") et un composant dans l'état "Ok". L'objectif de cette action est de remettre en service la fonction supportée initialement par le composant atteint en la faisant supporter par le composant "Ok". Elle peut être de 2 types. La reconfiguration de Type 1 est applicable dans le cas d'un composant capable de supporter une autre fonction principale (fonction régénérée initialement supportée par d'autres composants) mais implique la perte de la fonction pour laquelle il a été conçu. La reconfiguration de Type 2 correspond aux composants susceptibles de supporter une fonction régénérée tout en continuant à assurer sa fonction principale. Dans ce cas, la reconfiguration peut entraîner une modification de la fiabilité et de la vulnérabilité du composant : le processus de dégradation peut être accéléré et l'utilisation pour une autre fonction peut conduire à une nouvelle exposition aux agressions. De manière générale, la reconfiguration fait passer le composant de l'état "Ok" à l'état "en reconfiguration".
B. 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 ; elle peut donc être envisagée après un état : 1. Panne ou 2. Détérioré. On suppose ici qu'un composant "Détruit" n'est plus accessible. Le dépannage d'un composant en panne conduit à l'état "régénéré 1" (les fonctions techniques ne sont pas atteintes), alors que le dépannage d'un composant détérioré conduit à l'état "régénéré 2".
C. L'échange : le composant est échangé soit avec un composant du lot de bord ou du soutien logistique (ELI). Cette action nécessite de pouvoir accéder au composant et de pouvoir réaliser les actions de pose et dépose (au sens de la maintenabilité). Cette action est donc envisageable si le composant est dans l'état "panne" uniquement. Un composant dans un état détérioré est supposé ne plus pouvoir supporter une opération de dépose. Après échange, le composant est supposé être à nouveau dans l'état "Ok".
Un atome de modélisation générique peut donc être défini pour représenter le comportment des composants (sous-systèmes) en présence de défaillance, de dommage et de régénération (c.f. figure 3).

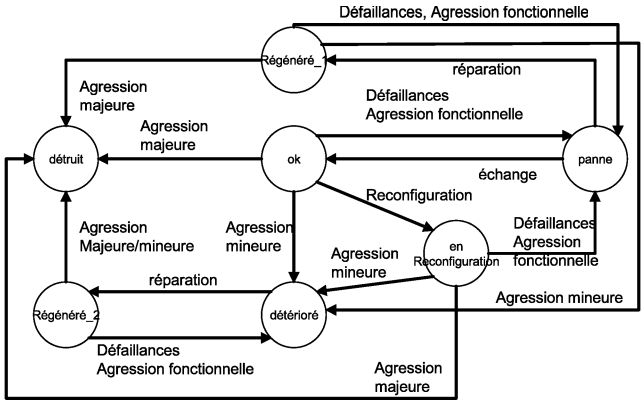

Fig. 3. Représentation du comportement en présence de défaillance, de dommage et de régénération

Dans l'exemple considéré dans ce papier, on suppose que le sous-système 5 qui supporte la 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 "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.
Dans la littérature, la distribution des temps de relatifs aux actions de maintenance est généralement exponentielle ou lognormale [8]. Dans une première approche, les transitions relatives aux actions de la régénération seront considérées comme déterministes.

IV. Modélisation SAN de l'atome de modélisation

Le formalisme (ou technique de modélisation) choisit pour représenter le comportement des sous-systèmes, des fonctions et l'agrégation (état des sous-systèmes vers état des fonctions) doit nous permettre de :

- prendre en compte les différentes interactions et dépendances entre les composants,
- modéliser des comportements de types "défaillance-dommage-régénération" complexes,
- considérer des comportements stochastiques particuliers définis par des distributions de probabilités générales (non-exponentielles),
- construire les modèles de manière intuitive, dans le respect des règles dérivées du modèle structurel relatif à la description hiérarchique des SdS,
- supporter une évaluation des performances de disponibilité par simulations, qui permettent de traiter les modèles de grands systèmes complexes avec différentes distributions de probabilités.

Le formalisme des Stochastic Activity Networks (SANs), a donc été choisi pour supporter le modèle dynamique. En effet, les SANs sont une extension des Réseaux de Petri stochastiques, incluant les réseaux de Petri stochastiques et les réseaux

de Petri stochastiques généralisés [17]. La puissance et la flexibilité des SANs permettent notamment de considérer des comportements stochastiques complexes avec des dépendances et des interactions entre les composants modélisés, et offrent la possibilité de traiter les modèles soit de manière analytique sur la base de la chaîne de Markov équivalente aux modèles dans le cas des systèmes Markoviens, soit par simulations de Monte Carlo, dans le cas de systèmes complexes avec des distributions de probabilités générales [18]. L'utilisation des SANs repose sur trois étapes : 1. la construction du modèle SAN, 2. la définition de variables de récompenses, 3. l'analyse du modèle.

A. Construction du modèle

Les SANs sont composés de trois éléments de base : des places, des activités et des *portes*. Les places sont utilisées pour représenter l'état du système et peuvent être connectées à des activités ou des *portes* par des arcs orientés. Les activités produisent des événements dans le modèle SAN qui représentent les changements d'état du système. Une distribution est associée à chaque activité qui détermine le taux de tir de l'activité. Enfin, les *portes* sont utilisées pour personnaliser le comportement par défaut des activités. Elles constituent l'élément qui fournit la puissance et la flexibilité nécessaire à la modélisation des systèmes complexes. Il y a 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* permettent de spécifier des conditions particulières pour permettre à l'activité d'être tirée alors que les *output gates* spécifient les fonctions de changement d'état personnalisées qui sont exécutées quand l'activité est tirée. Le modèle SAN d'un sous-système construit sur la base de la représentation conceptuelle (figure 3) est donné à la figure 4, partie gauche. Sur la base de cet atome générique (figure 3), les mécanismes de construction issus du modèle structurel permettent de définir les modèles SAN de chacun des composants avec ces caractéristiques propres. Par exemple, la possibilité pour le sous-système 5 de permettre une reconfiguration de la fonction OBS2 en remplaçant le sous-système 4 (régénération définie au niveau du modèle structurel relativement à l'axe des interactions) conduit à la présence des places "panne SSYST 4" et "detruit SSYST 4" utilisées pour le tirage de la transition "en reconfiguration" dans le modèle SAN du sous-système 5. Un modèle SAN est également construit

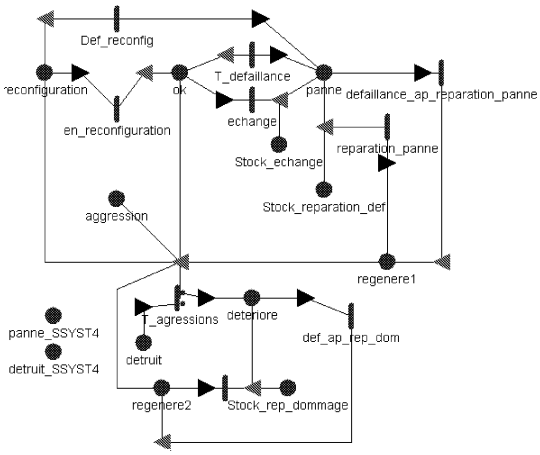

Fig. 4. Modèle SAN d'un sous-système 5 (SSYST 5)

pour les fonctions (figure 4, partie droite), dans lequel se trouvent les différents états des composants supports utilisés par les règles d'agrégation introduites au niveau des *input gates*. Enfin, la structure globale du SdS est donnée par un *Composed Model*, où sont définis les différents partages de places qui régissent les dépendances et les interactions entre les composants et les fonctions.

B. Définition des variables de récompenses

La seconde étape correspond à la définition des variables de récompenses qui représentent ici la disponibilité du système. Ces variables sont évaluées à partir d'une fonction qui calcule une valeur numérique basée sur l'état du système. La disponibilité globale du SdS sera donc donnée par une fonction qui attribue la valeur 1 à la variable *Dispo_op* si les trois fonctions OBS1, OBS2 et FEU sont soit dans l'état "Nominal", soit dans l'état "Dégradé". Cette variable sera évaluée sur une période de [0 - 24] unités de temps.

C. Simulations et Résultats

Le modèle complet du SdS a été construit et des simulations ont été réalisées. La fonction de répartition de la disponibilité pour chacune des simulations est reportée à la figure 6. Dans le premier cas, le modèle a été paramétré sans agression et aucune régénération n'est possible, seule la fiabilité du système intervient. La probabilité de réussite de la mission représentée par la probabilité que la disponibilité exprimée en heures soit supérieure à 95% du temps total de la mission (soit 22.8 heures) est de 0.973. Si l'agression "missile" est introduite (probabilité d'occurrence de 0.8), la probabilité de réussite de la mission n'est plus que de 0.05 si aucune régénération n'est possible. Cela met en

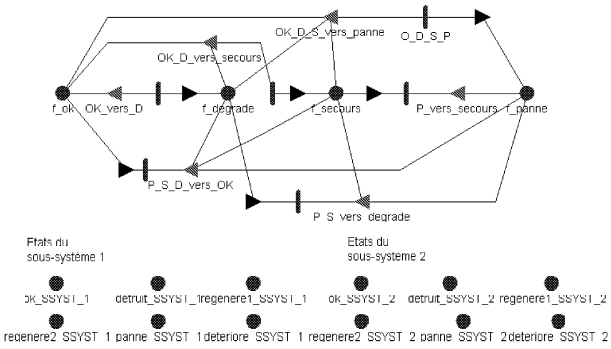

Fig. 5. Modèle SAN de la fonction OBS (OBS 1)

évidence l'importance de l'effet des agressions sur la disponibilité opérationnelle, la considération des agressions est donc indispensable dans l'évaluation de la disponibilité opérationnelle au combat. Enfin, avec la reconfiguration définie à la section III-C, la capacité du système à recouvrer des capacités opérationnelles garantit la réussite de mission avec une probabilité de 0.63.

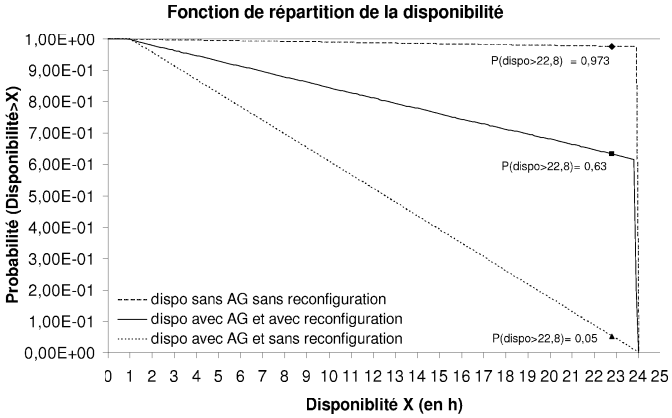

Fig. 6. Résultats

V. Conclusion

Ce papier traite du problème de l'évaluation de la disponibilité opérationnelle des systèmes et plus particulièrement des systèmes d'armes terrestres. Évoluant dans un contexte opérationnel hostile en présence de menaces, ces systèmes sont sujets en plus des défaillances, aux dommages subis au combat et nécessitent de recouvrer des capacités fonctionnelles par des actions de régénération pour terminer leur mission. Nous avons montré comment la considération des dommages et de la régénération en plus des défaillances impliquait la mise en oeuvre de nouveaux états dans les modèles de SdF. Basée sur une représentation par SANs, la modélisation bénéficie d'une grande flexibilité et permet l'évaluation par simulation de Monte Carlo, adaptée au cas de grands systèmes non-markoviens.
La faisabilité de la démarche ainsi que l'impact de la régénération des systèmes sur leur disponibilité opérationnelle ont été montrés au travers d'un exemple développé avec NEXTER et la DGA. Sur la base de cet exemple une mise à l'échelle du problème (une vingtaine de plates-formes représentées chacune par une vingtaine de composants) basée sur une architecture de SdS futurs prévue à l'horizon 2015 sera réalisée.

Références

[1] P. Tarvainen. Survey of the survivability of IT systems. In *Proceedings of the Ninth Nordic Workshop on Secure IT Systems*, pages 15–20, Helsinki, University of Technology, 4-5 Nov. 2004.

[2] G. Levitin and A. Lisnianski. Optimizing survivability of vulnerable series-parallel multi-state systems. *Reliability engineering and System Safety*, 79(3) :329–331, 2003.

[3] C. B. Campbell and D. W. Starbuck. Methodology for predicting recoverability. In *ASNE Reconfiguration and Survivability Symposium 2005 (RS 2005)*, Jacksonville/Mayport Area, February 16-18 2005. Amercian Society Naval Engineers.

[4] Y. Dutuit, E. Chatelet, J-P. Signoret, and P. Thomas. Dependability modeling and evaluation by using stochastic petri nets : application to two cases. *Reliability Engineering and System Safety*, 55(2) :117–124, 1997.

[5] M. Malhotra and K. S. Trivedi. Dependability modeling using petri-net based model. *IEEE Transactions on Reliability*, 38(3) :428–440, Setember 1995.

[6] Alexandre Muller, Marie-Christine Suhner, and Benoît Iung. Formalisation of a new prognosis model for supporting proactive maintenance implementation on industrial system. *Reliability Engineering & System Safety*, In Press, Corrected Proof, 2006.

[7] RESS. Dependent failure analysis - special issue. *Reliability Engineering and System Safety*, 34(3), 1991.

[8] K. S. Upadhya and N. K. Srinivasan. System simulation for availability of weapon systems under various missions. *Systems Engineering*, 8(4) :309–322, October 2005.

[9] Department of Defense. Mil-std-1629a military standard procedures for performing a failure mode, effects and criticalityanalysis. MIL-STD 1629A, Department of Defense, Washington, DC 20301, 24 NOVEMBER 1980 1980.

[10] Y. Liu, V. B. Mendiratta, and Kishor S. Trivedi. Survivability analysis of telephone access network. In *Proceedings of the 15th IEEE Internationnal Symposium on Software Engineering (ISSRE'04)*, Saint Malo, Bretagne, FRANCE, November 2004.

[11] J. Perrin, P. Esteve, and X. Le Vern. Régénération des matériels au combat. Étude prospective technico-opérationnelle, Délégation Générale pour l'Armement, (DGA), 2001.

[12] L. Barraco. La bulle opérationnelle aéroterrestre. *La jaune et la rouge*, pages 19–24, Mai 2006.

[13] M. Monnin, O. Senechal, B. Iung, P. Lelan, and M. Garrivet. A unified failure/damage approach to battle damage regeneration : Application to ground military systems. In *Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2006*, pages 379 – 384, Beijing, P R. CHINA, 29th August - 1st September 2006. IFAC.

[14] G. Guzie. Vulnerability risk assessment. Technical Report ARL-TR-1045, Army Research Laboratory, June 2000.

[15] Stanag 2418 battle damage repair policy. Technical report, NATO, December 1994.

[16] A. Toguyéni, P. Berruet, and E. Craye. Models and algorithms for failure diagnosis and recovery in fmss. *The International Journal of Flexible Manufacturing Systems*, 15 :57–85, 2003.

[17] W.H. Sanders and J.F. Meyer. Stochastic Activity Networks : Formal Definitions and Concepts. *Lecture Notes in Computer Science*, 2090 :315, 2001.

[18] S.T. Beaudet, T. Courtney, and W. H. Sanders. A behavior-based process for evaluatingh availability achievement risk using stochastic activity networks. In *Proc. of the 52nd Annual Reliability and Maintainability Symposium (RAMS2006)*, 2006.