Modélisation et évaluation de la disponibilité d'un système de signalisation ferroviaire ERTMS niveau 2

Siqi Qiu, Mohamed Sallak, Walter Schön, Zohra Cherfi

Modélisation et évaluation de la disponibilité d'un système de signalisation ferroviaire ERTMS niveau 2

Siqi Qiu, Mohamed Sallak, Walter Schön
Université de Technologie de Compiègne,
UMR CNRS 7253, Heudiasyc, France
Email : {siqi.qiu, mohamed.sallak, walter.schon}@utc.fr

Zohra Cherfi
Université de Technologie de Compiègne,
UMR CNRS 7337, Roberval
Email : zohra.cherfi@utc.fr

***Résumé*—Dans ce papier, on propose dans un premier temps la modélisation d'un système de signalisation ferroviaire ERTMS niveau 2 en utilisant les Statecharts. Ensuite, on propose l'évaluation de performances de ce système en termes de disponibilité et de temps moyen passé dans chaque état (mode de fonctionnement nominal, mode dégradé et mode de défaillance). L'originalité de ce travail réside dans la tentative de modélisation de tout le système de signalisation ERTMS niveau 2 en le considérant comme un Système de Systèmes. En outre, les facteurs humains ainsi que les défaillances réseaux sont aussi pris en compte dans le modèle proposé.**

***Index Terms*—Système-de-Systèmes (SdS), Statechart, ERTMS, ETCS, Disponibilité, Facteur humain, Défaillances réseaux.**

I. Introduction

La modélisation et l'évaluation de la disponibilité des systèmes complexes sont des tâches importantes dans le processus de conception sûre de ces systèmes. Dans ce papier, on propose de modéliser un système de signalisation ferroviaire ERTMS niveau 2 en le considérant comme un Système-de-Systèmes (SdS). Un SdS peut être vu comme un système se composant de systèmes indépendants, autonomes et complexes qui coopèrent pour atteindre un objectif commun. L'intérêt de considérer le système de signalisation ferroviaire comme un SdS réside dans le fait que cette approche permet d'avoir une vue globale du système de signalisation qui tient compte des systèmes qui constituent le système de signalisation ainsi que les différentes relations et interactions entre ces systèmes.

Récemment, la notion de SdS a connu un intérêt croissant de la part des chercheurs. En particulier, Jamshidi *et al.* ont démontré l'intérêt de l'utilisation de la notion de SdS dans la conception des grands systèmes [1], [2]. D'autres travaux de modélisations ont aussi apparu dans le domaine de modélisation des SdSs [3], [4]. Cependant, les SdSs n'ont pas de définition universelle. Dans ce papier, nous proposons la définition suivante :

Un SdS est un ensemble complexe qui [5] :

- se compose de parties complexes, indépendantes dont les niveaux d'interopérabilité élevés leur permettent d'avoir différentes configurations ;
- est caractérisé par la complexité contextuelle qui affecte son comportement ;
- a des limites ambiguës et changeantes ;
- présente des propriétés émergentes.

Plusieurs méthodes ont été proposées pour la modélisation des SdSs comme les modèles multi-agents, les réseaux bayésiens, les réseaux de Petri colorés, etc. Dans cette étude, on a choisi les Statecharts qui présentent une solution au problème de l'explosion combinatoire qui limite l'usage des automates à états finis. En effet, l'avantage des Statecharts est qu'ils rendent possible une décomposition hiérarchique de la notion d'état et donc ils permettent d'éviter un problème de combinatoire, dès lors que le système à modéliser est constitué de plusieurs sous-systèmes concurrents. On n'utilise pas l'arbre de défaillances à modéliser notre système, parce que l'arbre de défaillances est une méthode statique et il ne décrit pas l'aspect dynamique de notre modèle.

Dans la littérature, deux principaux types de structures ont été proposés pour modéliser les SdSs [6], [1]. La première est une structure hiérarchique. La deuxième est une structure relationnelle qui montre non seulement la composition du SdS mais aussi les relations entre les différentes parties. Notons, qu'à notre connaissance, il n'existe pas de travaux qui visent à modéliser le système de signalisation ferroviaire ERTMS niveau 2 avec toutes ses composantes (matériels, humains, réseaux, etc.) en tant que SdS. C'est pourquoi on propose, dans ce papier, de modéliser le système de signalisation ferroviaire sous forme de SdS. Des attributs de la Sûreté de Fonctionnement (SdF) seront utilisés pour évaluer la performance du SdS. En outre, les facteurs humains et les défaillances réseaux qui sont rarement modélisés quantitativement (c'est-à-dire en intégrant leurs taux d'occurrences) dans les systèmes de signalisation ferroviaires seront aussi pris en compte.

II. Système de signalisation ferroviaire

A. Description sommaire de l'ERTMS

Le système européen de surveillance du trafic ferroviaire (ERTMS) a été introduit pour garantir l'interopérabilité entre des différents pays et fabricants en créant un standard européen pour les systèmes de contrôle-commande des trains. Il est constitué de deux composants : le système

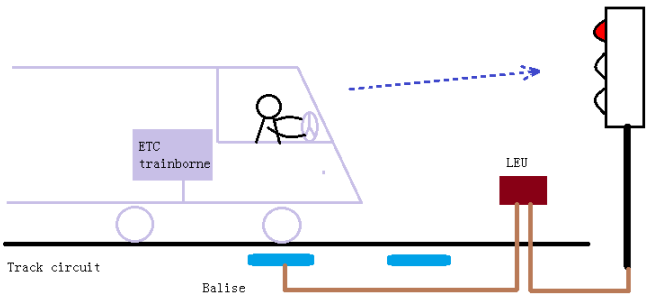

FIGURE 1. Architecture de l'ERTMS/ETCS niveau 1

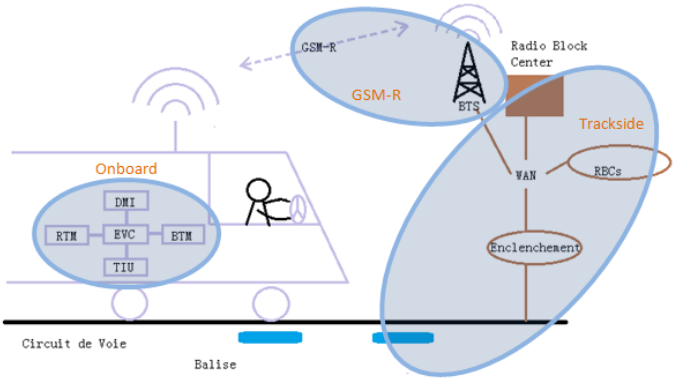

FIGURE 2. Architecture de l'ERTMS/ETCS niveau 2

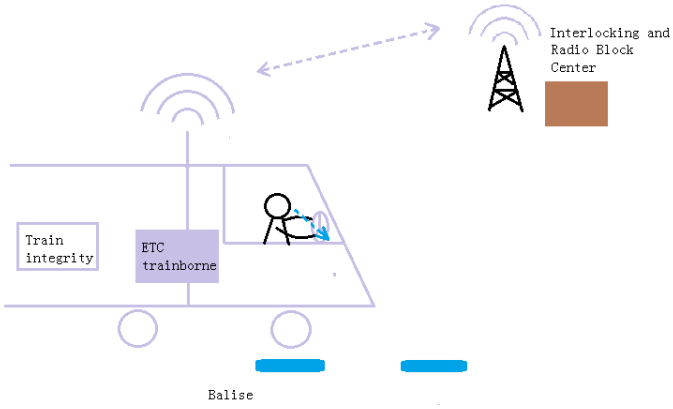

FIGURE 3. Architecture de l'ERTMS/ETCS niveau 3

européen de contrôle des trains (ETCS) et le GSM-R qui est un standard de communication sans fil basé sur le GSM pour les applications et les communications ferroviaires.

L'ETCS comporte trois niveaux. Les ETCSs niveau 1 et niveau 2 sont appliqués largement en Europe et en Asie. L'ETCS niveau 3 est encore en phase de développement. Dans l'ETCS niveau 1, la transmission d'informations du sol au train dépend totalement des balises qui sont installées sur le sol. Le conducteur conduit le train en fonction des signaux latéraux (cf. Figure 1). Dans l'ETCS niveau 2, les informations sont transmises par radio. La description des voies est affichée directement dans la cabine pour le conducteur, de sorte que les signaux latéraux ne sont plus nécessaires. Les balises aident le train à déterminer et à corriger sa position. Des circuits de voie permettent de suivre la position du train dans le système de signalisation ferroviaire français (cf. Figure 2). Dans l'ETCS niveau 3, la vérification de l'intégrité du train se fait par le train lui-même, donc les circuits de voie ne sont plus nécessaires. Les balises sont utilisées pour mettre à jour des informations de position et transmettre les données par GSM-R (cf. Figure 3).

Peu de travaux ont été proposés pour modéliser les plateformes ferroviaires dans le cadre de l'ERTMS. L'outil StoChart a été appliqué à la modélisation d'un ETCS afin d'évaluer sa fiabilité [7]. Une approche de type AMDEC (l'analyse des modes de défaillance, de leurs effets et de leur criticité) a été proposée pour l'optimisation de la fiabilité d'un système de signalisation ferroviaire [8]. Lalouette *et al.* ont proposé une approche basée sur les réseaux de Petri colorés afin d'évaluer la fiabilité d'un système de signalisation ferroviaire [9]. Des attributs de la SdF ont aussi été utilisés pour évaluer les solutions proposées par des services de localisation basées sur le satellite dans l'ERTMS [10].

B. Description du système de signalisation ferroviaire

Dans ce papier, on considère uniquement l'ERTMS/ETCS niveau 2 dont l'architecture est représentée dans la Figure 2 [11]. Il se compose de trois parties : le système Onboard, le système Trackside et le système GSM-R.

Le système Onboard est embarqué dans le train et sert à contrôler les mouvements du train. Il reçoit l'information provenant du système Trackside pour créer une "courbe de freinage". Le train doit respecter ce profil de vitesse afin de ralentir ou freiner avant les signaux d'arrêt ou d'urgence. Il reçoit également des messages provenant des balises et envoie des données qui décrivent par exemple la position du train et le mode d'opération au système Trackside via le GSM-R. Dans le système Onboard, on considère en particulier les composants suivants :

- RTM (Radio Transmission Module) fournit une interface bidirectionnelle avec le système Trackside par un terminal mobile.
- BTM (Balise Transmission Module) est une interface qui reçoit des messages provenant des balises et fournit l'énergie aux balises.
- TIU (Train Interface Unit) fournit une interface bidirectionnelle avec l'équipement du train.
- DMI (Driver Machine Interface) fournit une interface bidirectionnelle avec le conducteur.
- EVC (European Vital Computer) est un système de calcul temps réel embarqué. Il traite les messages des balises et mesure la vitesse et la position du train pour créer la "courbe de freinage".

Si le conducteur ne parvient pas à réaliser une opération

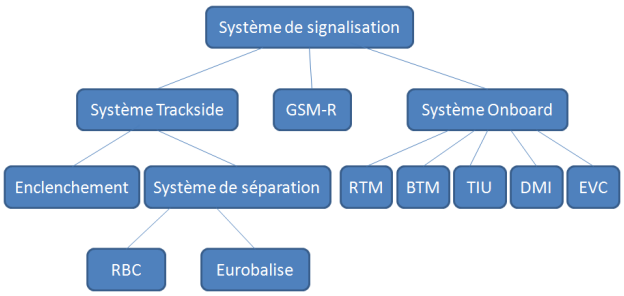

FIGURE 4. Structure hiérarchique

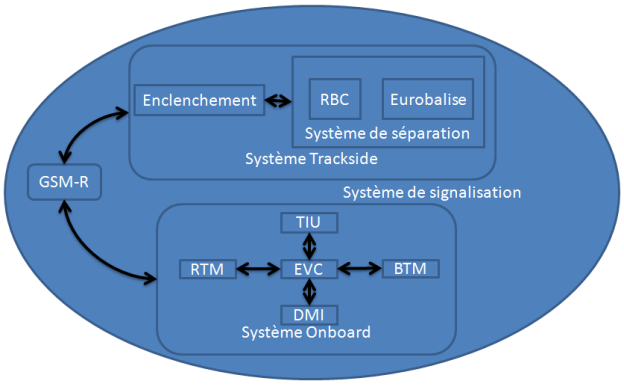

FIGURE 5. Structure relationnelle

correcte à temps, le système Onboard utilise automatiquement la procédure de freinage.

Le système Trackside sert à tracer des itinéraires, collecter l'état d'occupation du circuit de voie, détecter la position du train et envoyer des profils de vitesse corrects au train. En particulier, l'enclenchement sert à tracer des itinéraires et collecter l'état d'occupation du circuit de voie. Le système de séparation est constitué des Radio Bloc Centers et des Eurobalises. Le RBC (Radio Bloc Center) envoie des messages au train et collecte des données qui proviennent de l'enclenchement. La balise envoie des messages de position au train.

Le GSM-R est un standard de communication sans fil basé sur le GSM pour les applications et les communications ferroviaires. Pour la direction "bord à sol", la fréquence des GSM-R Messages se situe entre 876 MHz et 880 MHz. Pour la direction "sol à bord", la fréquence des GSM-R messages est entre 921 MHz et 925 MHz.

Il est clair que ce système de signalisation ferroviaire peut être considéré comme un SdS composé des trois systèmes Onboard, Trackside et GSM-R pour les raisons suivantes :

- les trois systèmes sont complexes, indépendants et autonomes.
- chaque système a son propre fonctionnement.
- les trois systèmes coopèrent pour atteindre un objectif commun.
- le système de signalisation ferroviaire montre également des propriétés émergentes. Il évolue au cours du temps et réagit aux différents cas imprévus.

Les Figures 4 et 5 donnent deux représentations possibles de ce SdS. La première est la structure hiérarchique et la deuxième est la structure relationnelle. La structure hiérarchique ne nécessite de spécifier que les échanges de données entre les trois systèmes alors que, dans la structure relationnelle, on est amené à spécifier aussi les échanges de données entre les différents composants des trois systèmes et donc notre modèle risque d'être très complexe. C'est pourquoi, dans ce papier, on adopte la structure hiérarchique.

III. Modélisation du système de signalisation par Statecharts

A. *Statecharts*

Les Statecharts sont des diagrammes comportementaux utilisant des états et des transitions pour décrire le comportement du système et de ses composants. Ils spécifient les séquences d'états par lesquels passe le système lors de l'occurrence des événements ainsi que les actions qui seront réalisées par la suite. On rappelle ici quelques notions fondamentales relatives aux Statecharts.

- Un **état** modélise une situation dans laquelle un système peut être.
- L'activité **entry** est un comportement optionnel qui est réalisé quand on entre dans l'état.
- L'activité **exit** est un comportement optionnel qui est effectué dès qu'on sort de l'état.
- L'activité **do** est un comportement optionnel qui est exécuté en étant dans l'état.
- Une **région** est une partie orthogonale d'un Statechart ou d'un état composite. Un Statechart ou un état composite peut contenir une ou plusieurs régions.
- Un **pseudo-état initial** n'est pas un vrai état. Il est un état intermédiaire et il est la source du Statechart dans une région. Chaque région dispose d'un et seulement un pseudo-état initial.
- Un **état final** est le dernier état d'une région.
- Une **transition** représente le passage instantané d'un état vers un autre.
- Un **événement** peut déclencher une transition.
- Une **condition** doit être satisfaite quand une transition est déclenchée.
- Une **action** spécifie un comportement optionnel à exécuter lorsque la transition est déclenchée.

L'intérêt de l'utilisation des Statecharts réside dans le fait qu'ils sont considérés comme étant des machines à états finis mais qui introduisent de nouvelles notions comme la hiérarchie d'états et les régions orthogonales ce qui permet d'éviter le problème de l'explosion combinatoire rencontré dans les automates à états finis. Ils étendent également les actions qui dépendent des états

avec des activités entry, do et exit.

Les Statecharts ont été peu utilisés dans les travaux de modélisation et d'évaluation de la SdF des systèmes ferroviaires. On trouve en particulier deux types d'applications des Statecharts : la première application est la modélisation des systèmes ferroviaires complexes. Dans [12], les Statecharts ont été utilisés pour modéliser un système d'enclenchement ferroviaire afin d'assurer la sécurité des voies pour les trains. La deuxième application est l'analyse des critères de sécurité. Deux représentations canoniques intermédiaires du Statechart qui conviennent à l'analyse des critères de sécurité sont introduites dans [13]. Des arbres de défaillance avec dépendances temporelles et des Statecharts temporisés ont été aussi introduits pour effectuer une analyse temporelle des propriétés de sécurité [14].

B. Intégration du facteur humain

L'erreur humaine peut être définie comme une faute de l'opérateur qui conduit à un accident ou un incident ferroviaire. Selon des statistiques publiées par la Federal Railroad Administration aux États-Unis [15], les facteurs humains sont les sources les plus importantes des accidents de train. En 2011, 36.35% des accidents ferroviaires aux États-Unis sont causés par des facteurs humains, 33.58% sont causés par des imperfections de la voie, 11.60% sont causés par des imperfections de l'équipement, 1.71% sont causés par des imperfections du signal et 16.77% sont causés par des causes diverses.

Dans la littérature, plusieurs travaux prenant en compte les facteurs humains ont été proposés. Dans le modèle proposé par Hudoklin and Rozman [16], la probabilité d'erreur humaine est considérée comme une mesure de la fiabilité humaine. La fatigue est considérée également comme un facteur important qui peut causer des accidents. Bien qu'elle soit difficile à mesurer, plusieurs méthodes d'analyse de la fiabilité humaine ont essayé de modéliser son effet [17]. Dans [18], un système assisté par ordinateur a été proposé afin d'analyser l'erreur humaine dans les systèmes ferroviaires. Ce système propose une hiérarchisation des causes de l'erreur humaine et des relations entre ces causes. Une méthode appelée APRECIH a été développée pour analyser des conséquences de la défiabilité humaine dans les systèmes ferroviaires critiques. Les dégradations des comportements humains ont été caractérisées par un modèle comportemental de la défiabilité humaine qui comporte trois facteurs comportementaux : des facteurs liés à l'acquisition, des facteurs liés à la solution des problèmes et des facteurs liés à l'action [19], [20]. Une étude énumérant la plupart des projets intégrant les facteurs humains dans le système ferroviaire a été réalisée dans [21]. L'identification des erreurs qui provoquent souvent l'occurrence des incidents et des accidents ferroviaires peut conduire à développer des stratégies de prévention comme ceux présentées par Baysari *et al.* [22], [23]. Notons que ces méthodes sont pour la plupart qualitatives sans aucune indication de modèles probabilistes pouvant être utilisé pour la quantification de l'erreur humaine.

Dans notre étude, on suppose que le taux d'erreur de l'opérateur λ_{op} est constant. La distribution appropriée pour le modèle de taux d'erreur constant est la distribution exponentielle. Donc le taux de transition de l'état de bon fonctionnement à l'état de défaillance est λ_{op}. Pour obtenir une valeur significative du taux d'erreur, on a considéré les statistiques publiées par la Federal Railroad Administration aux États-Unis de 2007 à 2011 [15]. Selon ces statistiques, il y a cinq facteurs humains qui influencent la performance humaine. Les cinq facteurs humains et les nombres d'accidents correspondants sur 107 lignes aux États-Unis sont donnés dans le tableau suivant :

	2011	2010	2009	2008	2007	Total
Absence de l'opérateur	74	63	53	91	101	382
Opérateur endormi	3	0	2	3	3	11
Affaiblissement à cause de médicament/alcool	0	1	0	0	1	2
Incapacité à cause de blessure/maladie	1	0	0	0	1	2
État physique de l'opérateur	1	0	0	0	1	2

Donc le taux d'erreur de l'opérateur sur chaque ligne est calculé de la manière suivante :

$\lambda_{op} = \frac{382+11+2+2+2}{5ans*107} = 8.514 * 10^{-5}\, h^{-1}$.

C. Intégration des défaillances réseaux

Le réseau de communication est également un facteur qui influence la performance du SdS. Dans la littérature, plusieurs méthodes d'analyse de la fiabilité des réseaux ont été proposées. Ces méthodes sont basées principalement sur les simulations de Monte-Carlo [24], [25], [26], [27]. Dans cette étude, on cherche à intégrer les défaillances réseaux dans notre Statechart.

Dans notre étude, on suppose que le taux de défaillance du réseau λ_r est constant. En outre, si le réseau tombe en panne, une réparation peut être effectuée donc le taux de transition de l'état de bon fonctionnement à l'état de défaillance est λ_r et le taux de transition de l'état de défaillance à l'état de fonctionnement est μ_r. Où $\mu_r = 0.6\, h^{-1}$ représente le taux de réparation. Pour obtenir une valeur significative du taux de défaillance du réseau, on a considéré les statistiques publiées par la Federal Railroad Administration aux États-Unis de 2007 à 2011 [15] où on trouve trois facteurs de défaillance des réseaux. Les trois facteurs et les nombres d'accidents correspondants sur 107 lignes aux États-Unis sont donnés dans le tableau suivant :

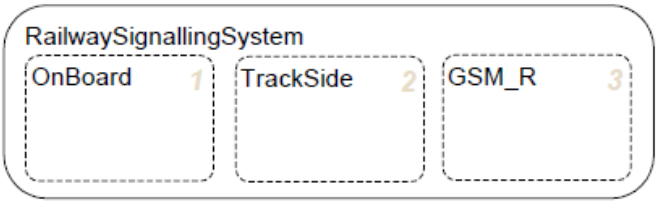

FIGURE 6. Statechart du SdS sous Stateflow

	2011	2010	2009	2008	2007	Total
Communication radio, échec à obéir	4	5	4	9	9	31
Comm. radio, échec d'envoi/réception	1	2	0	4	4	11
Télécommande, perte de comm	1	0	0	1	0	2

D'après le tableau ci-dessus, le taux de défaillance du réseau sur chaque ligne est
$\lambda_r = \frac{31+11+2}{5ans*107} = 9.3885 * 10^{-6}\, h^{-1}$.

D. Modélisation sous Stateflow

Stateflow est une toolbox de Simulink qui est l'outil de MATLAB dédié à la simulation du fonctionnement des systèmes. Stateflow fournit un environnement pour modéliser des systèmes par des Statecharts dans un modèle Simulink. La Figure 6 représente le Statechart du SdS complet. Les Figures 7, 8 et 9 montrent les Statecharts des trois systèmes qui composent le système de signalisation ferroviaire ERTMS niveau 2. Les Statecharts décrivent la communication entre le système Onboard et le système Trackside via GSM-R en présence de dégradations et de défaillances. Comme le montre les quatre Statecharts, le SdS se compose de trois systèmes : le système Onboard, le système Trackside et le système GSM-R qui collaborent en parallèle.

Tout d'abord, les trois systèmes entrent dans l'état "**Waiting**". Si la variable "Start" est vraie, tous les systèmes passent dans l'état "**Normal**". Au début, le système Onboard est dans l'état "**Calculation**", le système Trackside est dans l'état "**CollectionInfoCalculation**" et le système GSM-R est dans l'état "**CollectMessage**". Quand un événement *SignalFromTrack* arrive et que la fréquence des GSM-R messages est supérieure à 900MHz, c'est-à-dire que le système Trackside envoie des informations au système Onboard, alors le système Onboard passe dans l'état "**Receive**", le système Trackside passe dans l'état "**Send**" et le système GSM-R entre dans l'état "**Track2Train**". Quand un événement *EndSendToTrain* arrive, le système Onboard rentre dans l'état "**Calculation**", le système Trackside rentre dans l'état "**CollectionInfoCalculation**" et le système GSM-R revient dans l'état "**CollectMessage**". Le système Onboard a un état dégradé. Quand une *opération* arrive, si l'opérateur est disponible, le système entre dans l'état "**OperationByOperator**", sinon le système entre dans l'état "**OperationByComputer**" qui est un sous-état de l'état "**Degraded_OnBoard**". Lorsque l'événement *EndOperation* survient, le système entre dans l'état "**Calculation**" si l'opérateur n'est pas disponible, sinon le système Onboard revient à l'état "**Normal**". Chaque système possède un état de défaillance. Cet état de défaillance est constitué de deux types de défaillances. Le premier est le "**ErrorStateOfNet**". Une variable "network_failed" sert à indiquer l'état du réseau. Elle est modélisée par un booléen, quand il prend la valeur "1", les systèmes entrent dans l'état "**ErrorState**". Quand cette défaillance est réparée (un événement *RepairNet* arrive), les systèmes entrent dans l'état "**CorrectState**". Le second est le "**OrderOfErrorOfNet**". Lorsque le contrôleur de la circulation ferroviaire constate une anomalie dans le réseau, il peut donner une instruction *ErrorTrain2Track* ou *ErrorTrack2Train* immédiatement pour interrompre le réseau et les systèmes entrent dans l'état "**OrderOfErrorOfNet**". Cette défaillance peut être réparée par des événements de réparation correspondants comme *RepairSend_OB*, *RepairReceive_OB*, *RepairSend_TS*, etc. Une fois que les deux défaillances sont réparées, les systèmes peuvent revenir dans l'état "**Normal**" ou "**Degraded**". Quand la variable "End" est vraie, tous les systèmes retournent dans l'état "**Waiting**".

IV. Simulation et évaluation des performances

Pour évaluer les performances du SdS, on doit enregistrer le temps que les systèmes passent dans chaque état lors de la simulation. Ainsi, chaque système a une variable dont la valeur indique l'état dans lequel le système est. Notre pas de simulation est donné par $\Delta t = 1\, h$. On donne la liste des événements et des variables ainsi que leurs taux de transition ou leurs probabilités :

- Probabilité de transition(Operation, EndOperation) = 0.95
- Probabilité de transition(SignalFromTrack, EndSendToTrain, SignalFromTrain, EndSendToTrack) = 0.4
- P(f < 900) = 0.5. La direction de communication est déterminée par la fréquence des GSM-R messages. On suppose que chaque côté a la même probabilité d'envoyer des messages à l'autre côté.
- Taux de transition(operator=0) = λ_{op}, où $\lambda_{op} = 8.514 * 10^{-5}\, h^{-1}$.
- Taux de transition(network_failed=1) = λ_{r1}, où $\lambda_{r1} = 9.3885 * 10^{-6}\, h^{-1}$.
- Taux de transition(RepairNet) = μ_{r1}, où $\mu_{r1} = 0.6\, h^{-1}$.
- Taux de transition(ErrorTrain2Track, ErrorTrack2Train) = λ_{r2}, où $\lambda_{r2} = 0.0001\, h^{-1}$.
- Taux de transition(RepairReceive_OB, RepairSend_OB, RepairReceive_TS, RepairSend_TS, RepairTrack2Train, RepairTrain2Track) = μ_{r2}, où $\mu_{r2} = 0.6\, h^{-1}$.

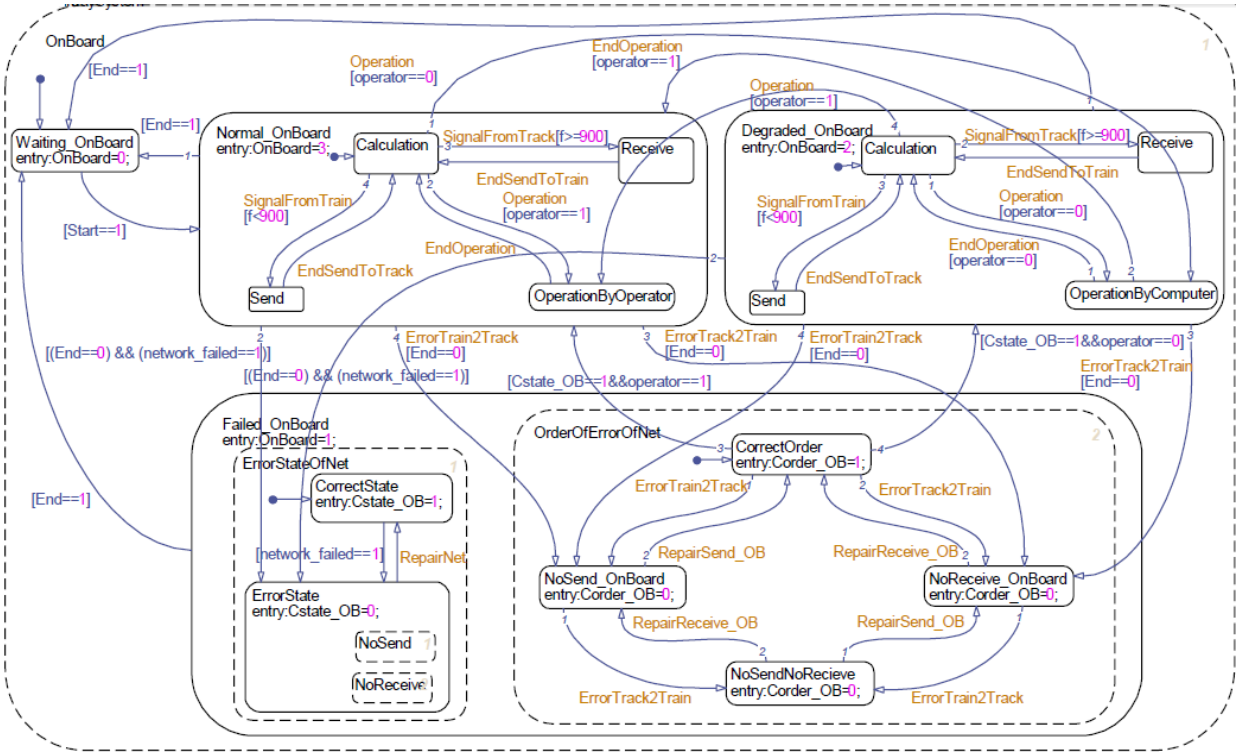

FIGURE 7. Statechart du système Onboard sous Stateflow

Pour le premier type "**ErrorStateOfNet**", on a

$$Taux\,de\,transition(Défaillance) = \lambda_{r1},\quad où\ \lambda_{r1} = 9.3885 * 10^{-6}\,h^{-1} \tag{1}$$

$$Taux\,de\,transition(Réparation) = \mu_{r1},\quad où\ \mu_{r1} = 0.6\,h^{-1} \tag{2}$$

Pour le deuxième type "**OrderOfErrorOfNet**", on a

$$Taux\,de\,transition(Défaillance) = \lambda_{r2},\quad où\ \lambda_{r2} = 0.0001\,h^{-1} \tag{3}$$

$$Taux\,de\,transition(Réparation) = \mu_{r2},\quad où\ \mu_{r2} = 0.6\,h^{-1} \tag{4}$$

Parmi des paramètres ci-dessus, le taux d'erreur de l'opérateur λ_{op} et le taux de défaillance du réseau λ_{r1} proviennent de la statistique. Pour les autres taux de transition, on a choisit des valeurs réalistes.

On réalise 100 simulations (temps d'échantillonnage : 1 heure, longueur de la simulation : 2 ans). Dans nos simulations, on trouve que les résultats de 100 simulations convergent. L'augmentation de nombre de simulation n'apporte pas un meilleur résultat. Donc, on prend 100 comme le nombre de simulation acceptable. La figure 10 représente le résultat d'une simulation. Elle montre les états de chaque système ainsi que l'état du SdS en fonction du temps. A chaque instant, l'état du SdS est déduit de

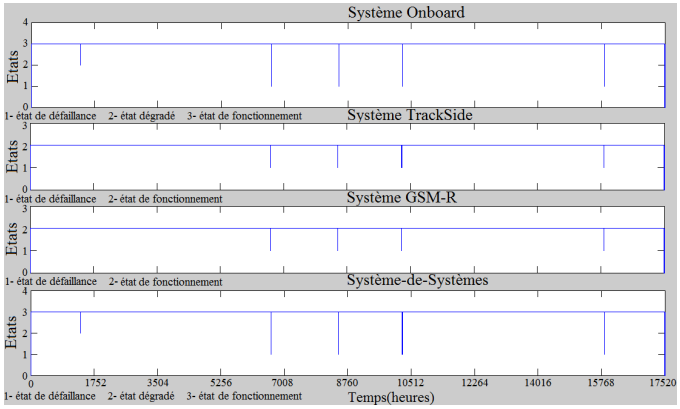

FIGURE 10. Résultat d'une seule simulation

l'état de ses trois systèmes. Le SdS a trois états : un état de fonctionnement, un état dégradé et un état de défaillance. Les attributs de la SdF sont généralement utilisés pour évaluer la performance du système. Dans cette partie, on propose le calcul de cinq paramètres : MUT (Durée moyenne de fonctionnement après réparation), MDT (Durée moyenne d'indisponibilité), MTTF (Temps moyen de fonctionnement avant panne), MTBF (Temps moyen entre pannes) et la disponibilité instantanée. Les moyennes sur 100 simulations des cinq paramètres sont présentées dans le tableau suivant :

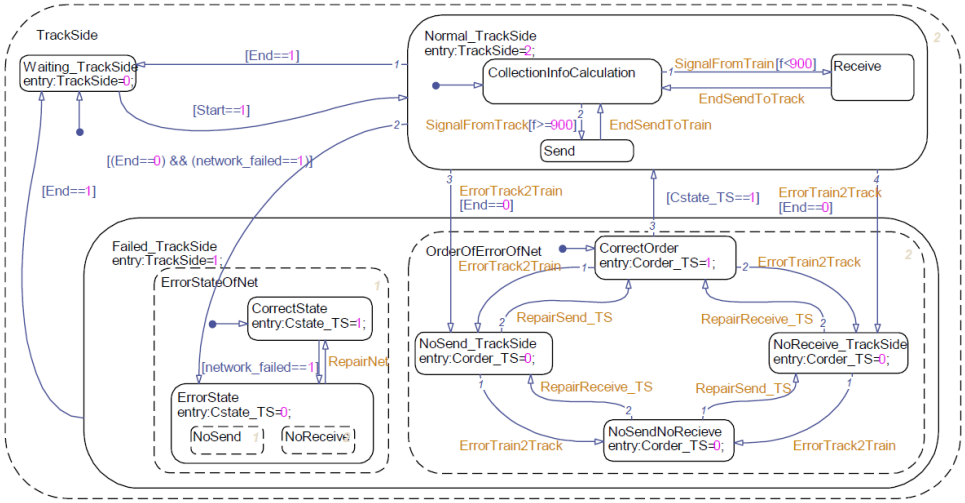

FIGURE 8. Statechart du système Trackside sous Stateflow

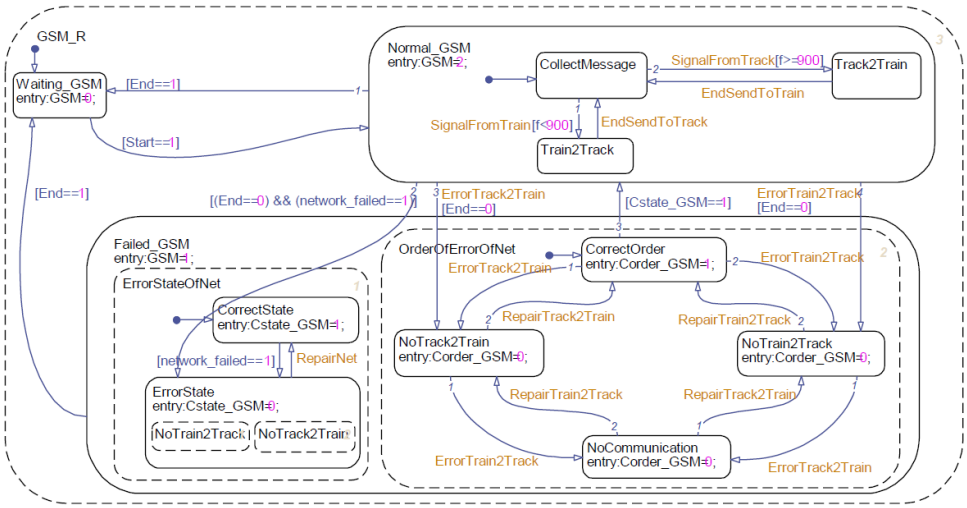

FIGURE 9. Statechart du système GSM-R sous Stateflow

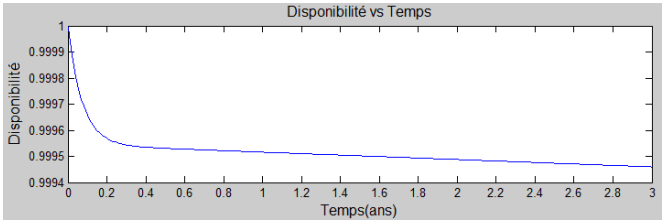

FIGURE 11. Disponibilité du SdS pendant trois ans

MUT	MDT	MTTF	MTBF	Disponibilité
4984.6h	2.6h	5626.4h	4987.2h	0.99949

La figure 11 montre la disponibilité instantanée du SdS sur une période de trois ans.

V. CONCLUSION

Dans cet article, on a proposé une méthode de modélisation et d'évaluation des performances d'un SdS représentant le système de signalisation ferroviaire ERTMS/ETCS niveau 2 avec prise en compte des facteurs humains et de défaillances réseaux. L'intérêt de l'approche SdS est d'avoir une vue globale du système de signalisation qui tient compte des systèmes qui constituent le système de signalisation ainsi que les différentes relations et interactions entre ces systèmes. Dans nos travaux futurs, on souhaite enrichir notre modèle, en introduisant la prise en compte de taux de défaillance et de réparation imprécis ainsi que des causes communes de défaillances.

RÉFÉRENCES

[1] M. Jamshidi, *Systems of Systems Engineering : Principles and Applications*. Taylor & Francis, 2008.

[2] T. Nanayakkara, M. Jamshidi, and F. Sahin, *Intelligent Control Systems with an Introduction to System of Systems Engineering*. Hoboken, USA : CRC Press, 2009.

[3] T. V. Huynh and J. S. Osmundson, "A Systems Engineering Methodology for Analyzing Systems of Systems Using the Systems Modeling Language (SysML)," in *2nd System of Systems Engineering Conference*, 2006.

[4] I. Eusgeld, C. Nan, and S. Dietz, ""System-of-systems" approach for interdependent critical infrastructures," *Reliability Engineering & System Safety*, vol. 96, no. 6, pp. 679–686, Jun. 2011.

[5] S. A. Sheard, "Systems of Systems Necessitates Bridging Systems Engineering and Complex Systems Sciences," in *2nd System of Systems Engineering Conference*, 2006.

[6] D. D. Walden, "System of Systems Engineering Leveraging COTS-Based Traditional Systems Engineering : Concepts and Analogies," in *2nd System of Systems Engineering Conference*, 2006.

[7] H. Hermanns, D. N. Jansen, and Y. S. Usenko, "From StoCharts to MoDeST : a comparative reliability analysis of train radio communications," in *Proceedings of the 5th international workshop on Software and performance, WOSP '05*. New York, USA : ACM Press, 2005, pp. 13–23.

[8] D. Vernez and F. Vuille, "Method to assess and optimise dependability of complex macro-systems : Application to a railway signalling system," *Safety Science*, vol. 47, no. 3, pp. 382–394, Mar. 2009.

[9] J. Lalouette, R. Caron, F. Scherb, N. Brinzei, A. Jf, and O. Malassé, "Performance assessment of european railway signalling system superposed of the french system in the presence of failures," in *17e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lamda-Mu'2010*, vol. 2, La Rochelle, France, 2010, pp. 2–9.

[10] J. Beugin and J. Marais, "Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization," *Transportation Research Part C : Emerging Technologies*, vol. 22, pp. 42–57, Jun. 2012.

[11] F. Flammini, *Model-based dependability evaluation of complex critical control systems*. Germany : VDM Verlag, 2009.

[12] M. Banci, A. Fantechi, and S. Gnesi, "The role of formal methods in developing a distribuited railway interlocking system," in *Proc. of the 5th Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems (FORMS/FORMAT 2004)*, E. Schnieder and G. Tarnai, Eds. Technical University of Braunschweig, Institute for Traffic Safety and Automation Engineering, 2004, pp. 220–230.

[13] Z. Pap, I. Majzik, A. Pataricza, and A. Szegi, "Methods of checking general safety criteria in UML statechart specifications," *Reliability Engineering & System Safety*, vol. 87, no. 1, pp. 89–107, Jan. 2005.

[14] J. Magott and P. Skrobanek, "Timing analysis of safety properties using fault trees with time dependencies and timed statecharts," *Reliability Engineering & System Safety*, vol. 97, no. 1, pp. 14–26, Jan. 2012.

[15] "Federal Railroad Administration Office of Safety Analysis." [Online]. Available : http ://safety-data.fra.dot.gov/officeofsafety/default.aspx

[16] A. Hudoklin and V. Rozman, "Reliability of railway traffic personnel," *Reliability Engineering & System Safety*, vol. 52, no. 2, pp. 165–169, May 1996.

[17] C. D. Griffith and S. Mahadevan, "Inclusion of fatigue effects in human reliability analysis," *Reliability Engineering & System Safety*, vol. 96, no. 11, pp. 1437–1447, Nov. 2011.

[18] D. S. Kim, D. H. Baek, and W. C. Yoon, "Development and evaluation of a computer-aided system for analyzing human error in railway operations," *Reliability Engineering & System Safety*, vol. 95, no. 2, pp. 87–98, Feb. 2010.

[19] F. Vanderhaegen, "APRECIH : a human unreliability analysis method - application to railway system," *Control Engineering Practice*, vol. 7, no. 11, pp. 1395–1403, Nov. 1999.

[20] ——, "A non-probabilistic prospective and retrospective human reliability analysis method - application to railway system," *Reliability Engineering & System Safety*, vol. 71, no. 1, pp. 1–13, Jan. 2001.

[21] J. R. Wilson and B. J. Norris, "Rail human factors : Past, present and future." *Applied ergonomics*, vol. 36, no. 6, pp. 649–660, Nov. 2005.

[22] M. T. Baysari, A. S. McIntosh, and J. R. Wilson, "Understanding the human factors contribution to railway accidents and incidents in Australia." *Accident Analysis and Prevention*, vol. 40, no. 5, pp. 1750–1757, Sep. 2008.

[23] M. T. Baysari, C. Caponecchia, A. S. McIntosh, and J. R. Wilson, "Classification of errors contributing to rail incidents and accidents : A comparison of two human error identification techniques," *Safety Science*, vol. 47, no. 7, pp. 948–957, Aug. 2009.

[24] J. E. Ramirez-Marquez and D. W. Coit, "A Monte-Carlo simulation approach for approximating multi-state two-terminal reliability," *Reliability Engineering & System Safety*, vol. 87, no. 2, pp. 253–264, Feb. 2005.

[25] J. E. Ramirez-Marquez and W. Jiang, "Confidence bounds for the reliability of binary capacitated two-terminal networks," *Reliability Engineering & System Safety*, vol. 91, no. 8, pp. 905–914, Aug. 2006.

[26] J. L. Cook and J. E. Ramirez-Marquez, "Two-terminal reliability analyses for a mobile ad hoc wireless network," *Reliability Engineering & System Safety*, vol. 92, no. 6, pp. 821–829, Jun. 2007.

[27] W.-C. Yeh, Y.-C. Lin, and Y. Y. Chung, "Performance analysis of cellular automata Monte Carlo Simulation for estimating network reliability," *Expert Systems with Applications*, vol. 37, no. 5, pp. 3537–3544, May 2010.