Projet Bonaventure
Livrable 2 : modèle des buts non-fonctionnels

Table des matières

I- Description de la méthodologie 2

II- Modélisation des buts non-fonctionnels 2

1- Hiérarchie principale : qualité de service 5

a) Identification des buts non-fonctionnels 5
b) Identification des buts de contribution 5
c) Impact des buts non-fonctionnels sur les buts fonctionnels 6
d) Illustration de la hiérarchie principale des buts non-fonctionnels 7

2- Hiérarchie secondaire : sécurité 8

a) Identification des buts non-fonctionnels 8
b) Identification des buts de contribution 10
c) Illustration du diagramme des buts non-fonctionnels de sécurité 14
d) Impact des buts non-fonctionnels sur les buts fonctionnels 15
e) Justification des modes de fonctionnement dégradés : modélisation des obstacles 16

Discussion 18

Références 19

I- Description de la méthodologie

SysML/KAOS est une méthode formelle d'ingénierie des exigences développée dans le cadre du projet FORMOSE (ANR-14-CE28-0009). Elle définit [1] :

- Un langage permettant de capturer les exigences fonctionnelles (ce qui doit être réalisé) et non fonctionnelles (contraintes de réalisation : sécurité, efficience, temporalité, etc.) d'un système sous forme de hiérarchies de buts.
- Un langage permettant de capturer les entités et les propriétés du domaine d'application du système.
- Des règles permettant de générer une spécification formelle à partir des modèles de buts et de domaine.
- Des règles permettant de propager les résultats/observations issus des activités de vérification et de validation formelle vers les modèles SysML/KAOS correspondants.

II- Modélisation des buts non-fonctionnels

La décomposition des buts non-fonctionnels se base sur les études réalisées par [2], [3] et [4]. Elle se focalise sur les exigences liées à la qualité de service du système.

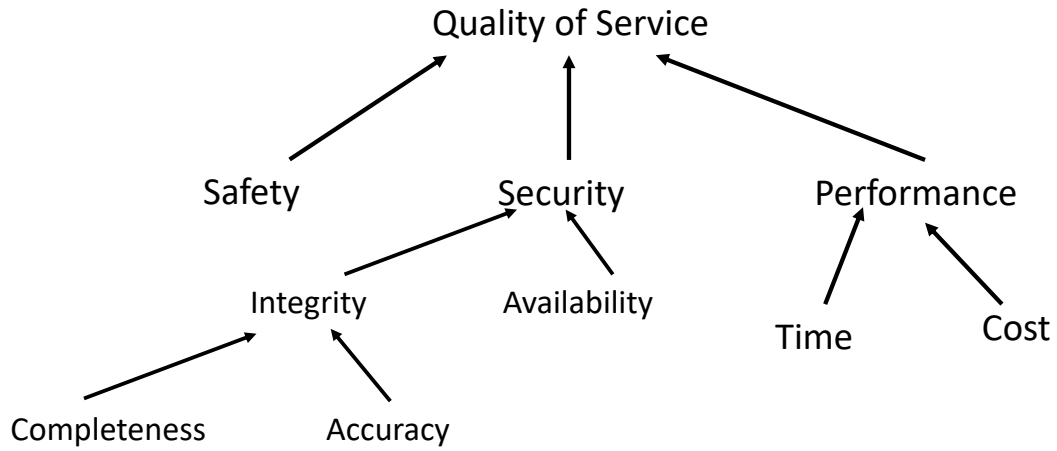

Figure 1 : Extrait de la taxonomie des types de buts non-fonctionnels (focus qualité de service) [3]

La Figure 1, construite à partir de [3], présente une hiérarchisation des types de buts non-fonctionnels qui contribuent à la qualité de service d'un système. Ainsi, pour maintenir une bonne qualité de service, il faut satisfaire les contraintes de sureté, de sécurité et de performance liées au fonctionnement du système :

- La satisfaction des contraintes de sécurité passe par celle des contraintes d'intégrité et de disponibilité :
  - Le plan de feux doit toujours être disponible. De plus, il doit être adapté à l'état du trafic, c'est à dire être le plus précis et le plus complet possible (la complétude ici s'associe au nombre de feux de signalisation dont l'état est défini par le plan de feux).
  - Les notifications à l'endroit des usagers relatives à l'état de la congestion et aux comportements recommandés doivent, dans la mesure du possible, être disponibles, précises et complètes (la complétude ici s'associe à la typologie des notifications adressées à l'usager : message « **congestion/circulation fluide** » vs visualisation géographique du « **positionnement des véhicules à la sortie du tunnel** », indication de la vitesse recommandée vs invitation à ralentir, etc.).
- La satisfaction des contraintes de performance passe par la satisfaction des contraintes de temps et de coût.

La hiérarchie des buts non-fonctionnels est construite dans un modèle différent de celui qui hiérarchise les buts fonctionnels. Toutefois, un troisième modèle dit modèle intégré permet de matérialiser l'impact des contraintes non-fonctionnels sur les objectifs fonctionnels du système [2]. L'impact peut conditionner la stratégie de raffinement des buts fonctionnels, peut conduire à l'apparition de nouveaux buts fonctionnels ou peut contraindre la façon dont un but fonctionnel élémentaire sera/doit être réalisé par le module auquel il est assigné.

Comme pour les buts fonctionnels, la hiérarchie des buts non-fonctionnels est construite par raffinements successifs de buts non-fonctionnels plus abstraits. Ainsi, l'opérateur AND apparaît lorsque plusieurs contraintes sont nécessaires pour satisfaire une contrainte de plus haut niveau. Lorsque plusieurs alternatives de satisfaction existent, c'est l'opérateur OR qui est utilisé. Les buts qui apparaissent au sommet de la hiérarchie des buts non-fonctionnels correspondent aux contraintes identifiées par les parties prenantes et conditionnant le fonctionnement du système à mettre en place. Chaque but non-fonctionnel est représenté par l'identifiant du type de contrainte qu'il désigne (voir Fig. 1) et par l'identifiant de l'entité du système sur laquelle la contrainte s'applique (eg : capteur, canal de communication, contrôleur). Chaque étape de raffinement permet de préciser les types des sous-contraintes qui composent une contrainte abstraite (voir Fig. 1) ou de préciser les sous-entités qui composent une entité abstraite. Le raffinement s'achève lorsqu'il est possible de proposer des solutions de satisfaction aux buts se situant au dernier niveau de la hiérarchie. Le raffinement d'un but non fonctionnel cesse également d'être nécessaire si la satisfaction de ce dernier ne suscite aucun intérêt ou s'il n'y a qu'une seule façon de le satisfaire (le raffinement ne va avoir aucun impact sur la mise en œuvre du système).

Chaque solution de satisfaction d'un (ou plusieurs) but(s) non-fonctionnel(s) élémentaire(s) est appelé **but de contribution** [2]. Chacune d'elles peut contribuer positivement (**++** ou **+**) ou négativement (**--** ou **-**) à la satisfaction d'un but non-fonctionnel élémentaire [3]. Pour des raisons de simplification et pour plus de clarté, lorsque la contribution existe mais qu'elle n'est ni totalement négative ni totalement positive, nous proposons l'utilisation de l'opérateur **+-** (fédère les opérateurs **HURT** et **HELP** proposés dans [3]). Ça peut par exemple être le cas lorsqu'un but de

contribution est construit en combinant un but à contribution positive et un autre à contribution négative. En cas de conflit (solution de satisfaction contribuant positivement à un but non-fonctionnel et négativement à un autre), il est nécessaire d'évaluer les priorités entre buts non-fonctionnels ou de considérer un autre but de contribution. Les buts de contribution peuvent avoir des impacts positifs ou négatifs sur des buts fonctionnels. L'impact d'un but de contribution **CG** sur un but fonctionnel **FG** est positif lorsque le choix de **CG** assure de façon quasi certaine que le système réalisera **FG** tout en satisfaisant les buts non-fonctionnels auxquels **CG** contribue positivement. L'impact est négatif lorsque le choix de **CG** peut compromettre la réalisation de **FG** ou lorsque la réalisation de **FG** risque de façon quasi certaine d'empêcher la satisfaction des buts non-fonctionnels auxquels **CG** contribue positivement.

1- Hiérarchie principale : qualité de service

a) Identification des buts non-fonctionnels

Niveau de raffinement	**Identification du but**	**Description**
0 (niveau racine)	*Quality of Service [System]*	Maintenir une bonne qualité de service.
1	*Safety [System]*	Garantir la sureté des usagers.
	Security [System]	Garantir la sécurité des données critiques pour le bon fonctionnement du système. Ce but est développé dans une autre hiérarchie dite secondaire.
	Performance [System]	Optimiser les performances du système.
2	*Time [System]*	Optimiser les délais de fonctionnement du système.
	Cost [System]	Optimiser les coûts de fonctionnement du système.
3	*Cost [Sensor]*	Optimiser les coûts de fonctionnement des capteurs utilisés pour la détection du niveau de trafic.
	Cost [Controller]	Optimiser les coûts de fonctionnement des contrôleurs en charge de la régulation du niveau de trafic.
	Cost [Actuator]	Optimiser les coûts de fonctionnement des actuateurs servant à interagir avec les usagers.

b) Identification des buts de contribution

Identifiant du but de contribution	**Description**	**Contribution**	
		Positive	Négative
AvoidCollisions	Éviter les collisions dues à la courbure du tunnel.	• *Safety [System]*	
UseAID	Utiliser l'AID (Automatic Incident Detector) du MTQ pour la détection du niveau de	• *Cost [Sensor]*	

	trafic à considérer pour déterminer le plan de feux et les notifications à l'attention des usagers.		
UseVdMCamera	Utiliser des caméras thermiques appartenant à la VdM pour la détection du niveau de trafic.	• *Cost [Sensor]*	
UseVdMRadar	Utiliser des radars de trafic appartenant à la VdM pour la détection du niveau de trafic.	• *Cost [Sensor]*	
UseGroundSensor	Utiliser des capteurs souterrains appartenant à la VdM pour la détection du niveau de trafic.		• Cost [Sensor] *(le capteur souterrain est difficilement maintenable et réutilisable, ce qui contribue à augmenter son coût de fonctionnement)*
UsePMV	Utiliser les panneaux à message variable pour la notification des usagers.		• Cost [Actuator] *(choisir d'utiliser des PMVs pour la notification des usagers requiert l'achat et la maintenance de ces derniers)*
UseWaze	Utiliser la plateforme Waze pour la notification des usagers.	• Cost [Actuator]	
UseGMaps	Utiliser la plateforme Google Maps pour la notification des usagers.	• Cost [Actuator]	

c) Impact des buts non-fonctionnels sur les buts fonctionnels

Comme le montre la Figure 2, le choix : (1) du but de contribution **AvoidCollisions** a un impact significatif sur la satisfaction du but fonctionnel **BringOutEachVehiclePresentInTunnel** du modèle des buts fonctionnels [5] et requiert la définition du but fonctionnel **BlockVehicleEntrance** (Bloquer l'entrée des véhicules dans le tunnel); (2) des buts de contribution **UseAID, UseVdMCamera, UseVdMRadar** et/ou **UseGroundSensor** a un impact significatif sur la satisfaction du but fonctionnel **DetermineTrafficLevel** ; et (3) des buts de contribution **UsePMV, UseWaze,** et/ou **UseGMaps** a un impact significatif sur la satisfaction du but fonctionnel **SuperviseTrafficLevel**.

d) Illustration de la hiérarchie principale des buts non-fonctionnels

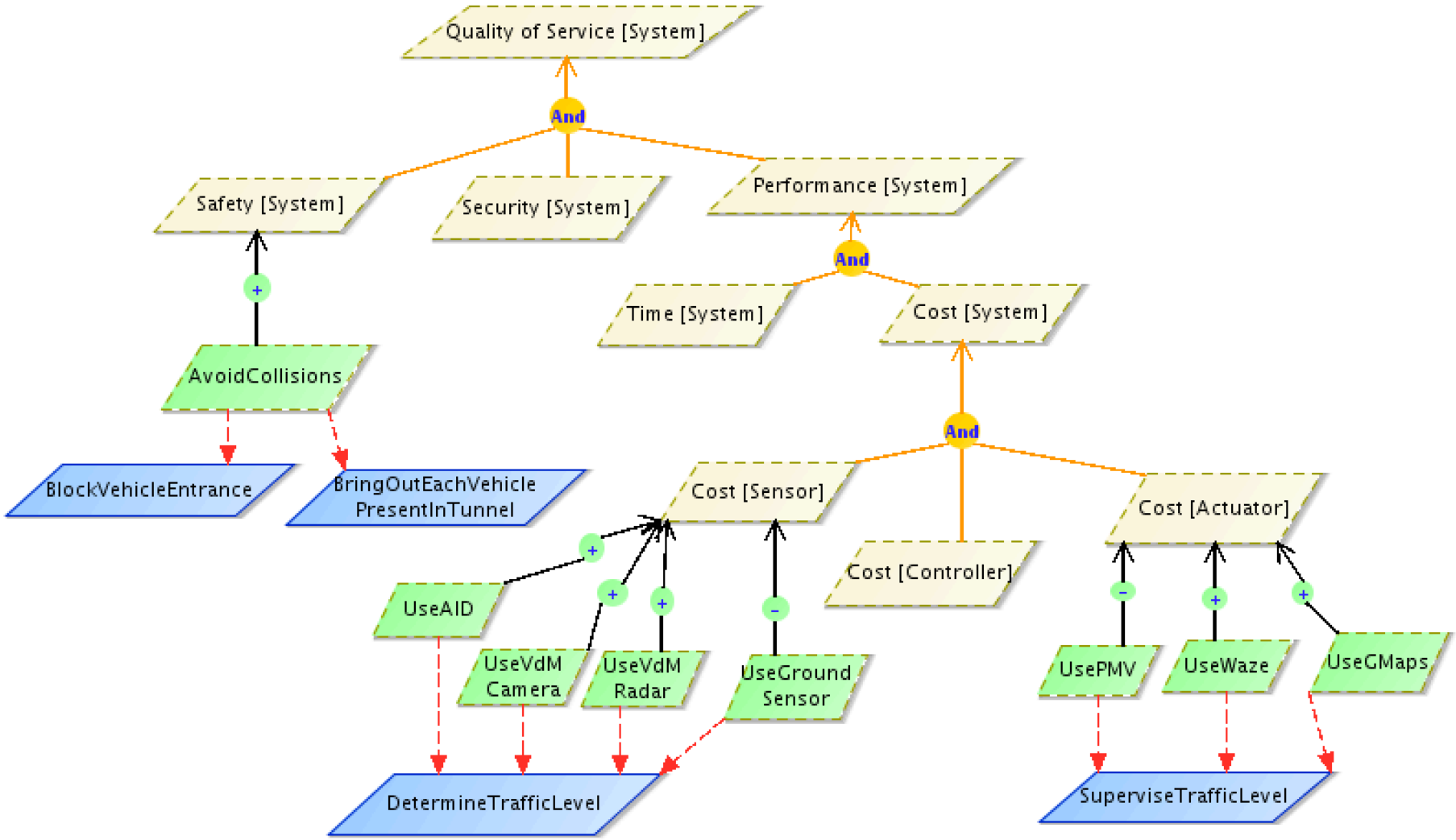

Figure 2: Hiérarchie principale des buts non-fonctionnels

2- Hiérarchie secondaire : sécurité

a) Identification des buts non-fonctionnels

Niveau de raffinement	**Identification du but**	**Description**
0 (niveau racine)	*Security [System]*	Garantir la sécurité des données critiques pour le bon fonctionnement du système. Pour assurer cette contrainte, nous identifions la nécessité de garantir l'intégrité et la disponibilité des données et modules permettant de contrôler la signalisation routière à la sortie du tunnel et de notifier l'usager (état de la circulation et comportements recommandés) [6]. L'hypothèse sous-jacente est que l'usager se conformera à la signalétique et aux recommandations qui lui sont adressées.
1	*Integrity [System]*	Garantir l'intégrité des données permettant de contrôler la signalisation routière à la sortie du tunnel et de notifier l'usager [6].
	Availability [System]	Garantir la disponibilité des données et modules permettant de contrôler la signalisation routière à la sortie du tunnel et de notifier l'usager [6].
2	*Integrity [TSP (TrafficSignalProgram)]*	Garantir l'intégrité du plan de feux [7]. Il est à noter que nous ne nous intéressons pas au module de régulation, car son fonctionnement est défini de façon permanente et n'est plus sujet à discussion (il est considéré comme faisant partie de l'environnement). Nous nous intéressons en revanche au module de supervision et donc à l'intégrité du plan de feux appliqué en cas de préemption de l'automate de régulation [8].
	Integrity [UN (UserNotification)]	Garantir l'intégrité des notifications adressées aux usagers par le centre de supervision [7].
	Availability [TL (TrafficLevel)]	Garantir que les mesures des capteurs sont disponibles et permettent effectivement d'obtenir une estimation de l'état réel du trafic [7]. Ce but dépend de la couverture (par rapport aux 4 zones d'intérêt [8]) et de la fréquence d'indisponibilité des capteurs sélectionnés. Par exemple, le Radar couvre les 4 zones, mais est parfois indisponible. En conséquence, il faut le combiner avec un autre capteur (caméra thermique ou capteur souterrain) afin de maximiser la satisfiabilité du but.
	Availability [TSPSupervision]	Garantir la disponibilité d'une supervision du plan de feux [7]. Le plan de feux est supposé toujours disponible et fourni par le module de régulation [8]. Nous nous intéressons donc à la

		disponibilité d'une supervision permettant de contrôler son adéquation par rapport à l'état réel du trafic.
	Availability [UN]	Garantir la disponibilité des notifications à adresser aux usagers et assurer leur diffusion [7].
3	*Integrity [TL-TSP]*	Garantir l'intégrité des données de trafic servant à la supervision du plan de feux [9].
	Integrity [SupersededTSP]	En cas de préemption de l'automate de régulation, garantir l'intégrité du plan de feux défini pour supplanter celui déterminé par l'automate [8].
	Integrity [TL-UN]	Garantir l'intégrité des données de trafic servant à déterminer les notifications à adresser aux usagers [9]. La décomposition de ce but ne figure pas dans la hiérarchie des buts non fonctionnels car, de notre compréhension actuelle du fonctionnement du CGMU et du CGIC, les contraintes sont identiques à celles modélisées par le but *Integrity [TL-TSP]*.
	Integrity [IssuedUN]	Garantir l'intégrité des notifications mises à la disposition des usagers [7].
	Availability [TSPSuperviser]	Garantir la disponibilité d'un superviseur chargé de contrôler l'adéquation entre le plan de feux déterminé par l'automate de régulation et l'état courant du trafic [8].
	Availability [TL-TSP]	Garantir la disponibilité des données de trafic auprès du superviseur de plans de feux.
	Availability [UNDisplayer]	Garantir la disponibilité des interfaces permettant de notifier les usagers (PMVs, équipements intelligents et applications requises, etc.) [7].
	Availability [UNSuperviser]	Garantir la disponibilité d'un module (automate mécatronique, logiciel, etc.) capable de déterminer les notifications à adresser aux usagers suivant l'état courant du trafic [7].
	Availability [TL-UN]	Garantir la disponibilité des données de trafic auprès du contrôleur chargé de déterminer les notifications à adresser aux usagers [7]. De notre compréhension actuelle, les contraintes relatives à ce but sont identiques à celles associées au but *Availability [TL-TSP]*.
4	*Accuracy [TL-TSP]*	Garantir la précision des données de trafic servant à superviser le plan de feux [9].
	Completeness [TLl-TSP]	Garantir la complétude des données de trafic servant à superviser le plan de feux [9].
	Accuracy [IssuedUN]	Garantir la précision des notifications mises à la disposition des usagers [7].
	Completeness [IssuedUN]	Garantir que les notifications adressées aux usagers soient suffisamment riches pour qu'en s'y référant, il soit possible de sortir du tunnel en toute sécurité [7].
	Accuracy [TL-UN]	Garantir la précision des données de trafic servant à déterminer les notifications à adresser aux usagers [9]. Il est à préciser que ce but ne figure pas dans la représentation de la hiérarchie des buts pour des raisons de clarté.
	Completeness [TL-UN]	Garantir la complétude des données de trafic servant à déterminer les notifications à adresser aux usagers [9]. Il est à préciser que ce but ne figure pas dans la représentation de la hiérarchie des buts pour des raisons de clarté.

b) Identification des buts de contribution

Identifiant du but de contribution	Description	Contribution	
		Positive	Négative
UseAID	Utiliser l'AID (Automatic Incident Detector) du MTQ pour la détection du niveau de trafic à considérer pour la supervision du plan de feux et la notification des usagers. Ceci revient à se limiter à la supervision en mode normal uniquement.	• Accuracy [TL-TSP] • Completeness [TL-TSP] • Accuracy [TL-UN] • Completeness [TL-UN] • Availability [TL]	• Availability [TL-TSP] *(l'usage de l'AID rend la satisfaction de ce but difficile parce que l'information de détection sera transmise au CIGC qui devra l'acheminer au CGMU ; or la liaison CIGC-CGMU n'est pas sûre)* • Availability [TL-UN]
UseVdMCamera	Utiliser uniquement la caméra thermique de la VdM pour la détection du niveau de trafic.	**Note : si après analyse et vérification il est avéré que ce but de contribution ne contribue positivement à aucun but non-fonctionnel, alors il devra être supprimé du modèle des buts non-fonctionnels.**	• Availability [TL] *(la caméra thermique ne couvre que ¼ de la portion d'intérêt du tunnel. De plus, elle est parfois indisponible. Par conséquent, elle ne peut à elle seule fournir une estimation exploitable de l'état du trafic)* • Accuracy [TL-TSP] *(l'usage des capteurs de la VdM ne permet pas d'atteindre le niveau de précision optimal (celui de l'AID))* • Completeness [TL-TSP] *(en utilisant uniquement la caméra thermique de la VdM, l'information obtenue n'est pas complète : lorsque l'information est disponible, elle ne concerne que ¼ de la portion d'intérêt du tunnel ; c'est pour cette raison que la VdM l'adjoint au radar)* • Accuracy [TL-UN] • Completeness [TL-UN] • Availability [TL-TSP] *(l'état du trafic ne peut être estimé de façon satisfaisante, donc cette*

			information ne peut être disponible pour la supervision du trafic) • Availability [TL-UN]
UseVdMRadar	Utiliser uniquement le radar de trafic de la VdM pour la détection du niveau de trafic.	• Completeness [TL-TSP] *(le radar couvre l'entièreté de la portion d'intérêt du tunnel)* • Completeness [TL-UN] • Availability [TL] *(contribution partiellement positive (en comparaison à l'AID) car le radar fournit une estimation du trafic sur l'entièreté de la portion d'intérêt du tunnel ; toutefois, il est parfois indisponible)* • Availability [TL-TSP] *(contribution partiellement positive (en comparaison à l'AID) car (1) la liaison VdMSensor-CGMU est plus sure que la liaison CGGMU-CIGC ; (2) lorsque le radar est disponible, l'information fournie permet d'estimer l'état du trafic sur l'entièreté de la portion d'intérêt du tunnel)* • Availability [TL-UN]	• Accuracy [TL-TSP] *(l'usage des capteurs de la VdM ne permet pas d'atteindre le niveau de précision optimal (celui de l'AID))* • Accuracy [TL-UN]
UseGroundSensor	Utiliser uniquement le capteur souterrain pour la détection du niveau de trafic.	**Note : si après analyse et vérification il est avéré que ce but de contribution ne contribue positivement à aucun but non-fonctionnel, alors il devra être supprimé du modèle des buts non-fonctionnels.**	• Availability [TL] *(ce capteur ne couvre que ¼ de la portion d'intérêt du tunnel. De plus, il est très souvent indisponible, ceci combiné au coût élevé associé à son exploitation)* • Accuracy [TL-TSP] *(l'usage des capteurs de la VdM ne permet pas d'atteindre le niveau de précision optimal (celui de l'AID))* • Completeness [TL-TSP] *(en utilisant uniquement ce capteur, l'information obtenue n'est pas complète : lorsque l'information est*

			disponible, elle ne concerne que ¼ de la portion d'intérêt du tunnel ; c'est pour cette raison que le capteur doit être adjoint au radar) • Accuracy [TL-UN] • Completeness [TL-UN] • Availability [TL-TSP] *(l'état du trafic ne peut être estimé de façon satisfaisante, donc cette information ne peut être disponible pour la supervision du trafic)* • Availability [TL-UN]
UseVdMRadar &Camera	Combiner la caméra thermique et le radar de trafic de la VdM pour détecter le niveau de trafic à transmettre au CGMU (et se limiter uniquement à cette combinaison). Ceci revient à se limiter à la supervision en mode dégradé I [8].	• Completeness [TL-TSP] *(le radar couvre l'entièreté de la portion d'intérêt du tunnel)* • Completeness [TL-UN] • Availability [TL] *(le fait d'adjoindre une caméra thermique au radar permet d'atteindre une disponibilité jugée suffisante)* • Availability [TL-TSP] *(contribution partiellement positive (en comparaison à l'AID) car la liaison VdMSensor-CGMU est plus sûre que la liaison CGGMU-CIGC)* • Availability [TL-UN]	• Accuracy [TL-TSP] *(l'usage des capteurs de la VdM ne permet pas d'atteindre le niveau de précision optimal (celui de l'AID))* • Accuracy [TL-UN]
UseVdMRadar &Camera&AID	Combiner l'usage de l'AID, de la caméra thermique et du radar. Ceci revient à considérer, par ordre de priorité, les modes de supervision normal et dégradé I.	• Accuracy [TL-TSP] *(contribution partiellement positive (en comparaison à l'AID) car le fait d'adjoindre l'AID aux capteurs de la VdM permet de rendre l'information exploitée suffisamment précise en fonctionnement normal, mais pas tout le temps)* • Accuracy [TL-UN] • Completeness [TL-TSP]	

		• Completeness [TL-UN] • Availability [TL] • Availability [TL-TSP] *(contribution partiellement positive car les liaisons utilisées, quel que soit le mode, ne sont pas suffisamment fiables ; toutefois, la redondance permet d'accentuer la fiabilité)* • Availability [TL-UN]	
UsePMV	Utiliser les panneaux à message variable pour la notification des usagers.	• Accuracy [IssuedUN] • Availability [UNDisplayer]	• Completeness [IssuedUN] *(un PMV ne permet d'afficher qu'une information partielle : la complétude ici s'associe à la typologie des notifications adressées à l'usager : message « congestion/circulation fluide » vs visualisation géographique du « positionnement des véhicules à la sortie du tunnel », indication de la vitesse recommandée vs invitation à ralentir, etc.)*
UseWaze	Utiliser la plateforme Waze pour la notification des usagers.	• Accuracy [IssuedUN] • Completeness [IssuedUN]	• Availability [UNDisplayer] *(impossible de garantir que l'usager aura le client Waze ou même qu'il sera en possession d'un terminal intelligent)*
UseGMaps	Utiliser la plateforme Google Maps pour la notification des usagers.	• Accuracy [IssuedUN] • Completeness [IssuedUN]	• Availability [UNDisplayer] *(impossible de garantir que l'usager aura le client GMaps ou même qu'il sera en possession d'un terminal intelligent)*

c) Illustration du diagramme des buts non-fonctionnels de sécurité

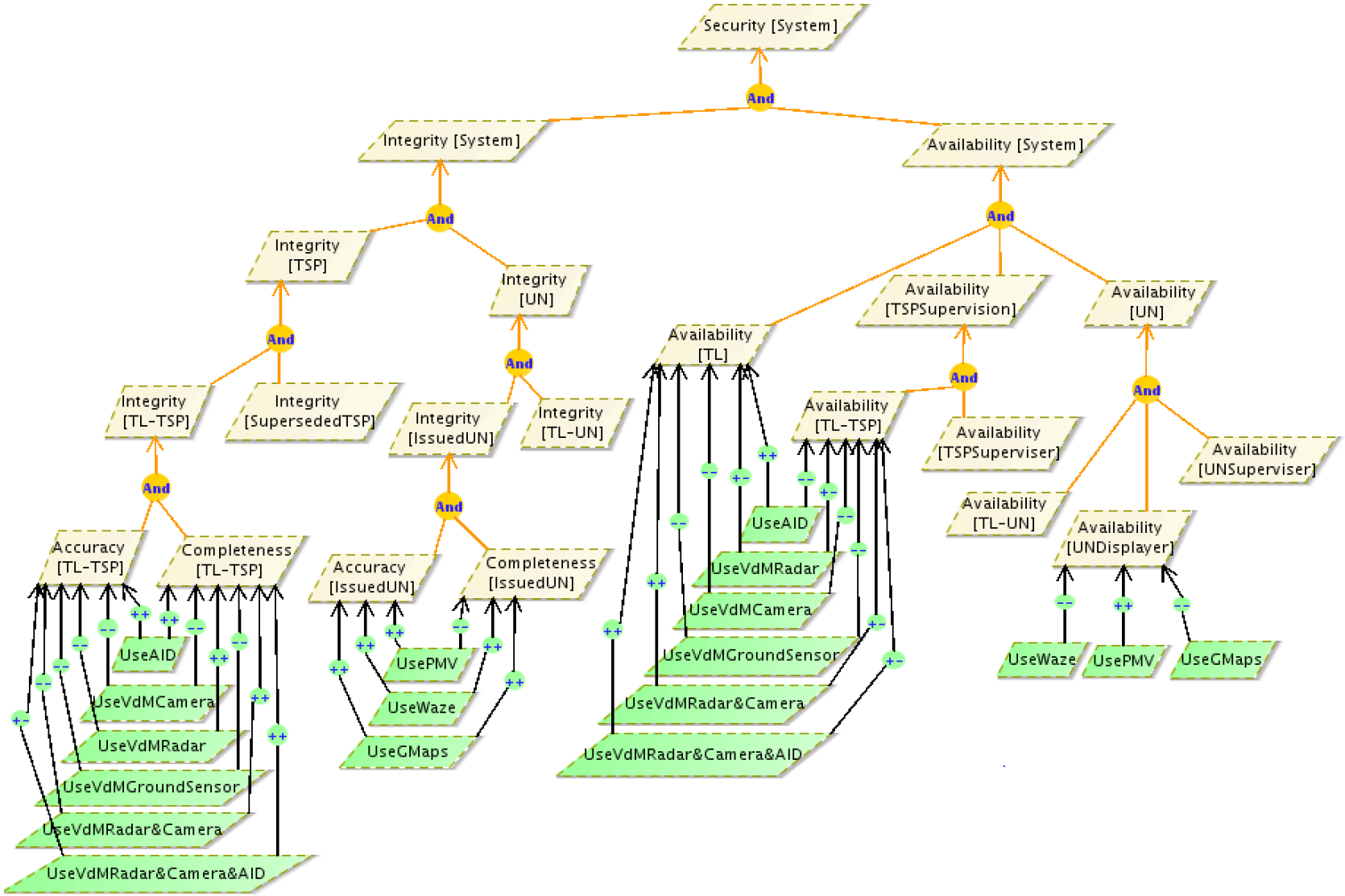

Figure 3: Diagramme des buts non-fonctionnels de sécurité

d) Impact des buts non-fonctionnels sur les buts fonctionnels

Pour cette partie, nous nous limitons au but de contribution **UseVdMRadar&Camera&AID** pour illustrer la façon de matérialiser l'impact du non-fonctionnel sur le fonctionnel. Il est question ici de présenter les conséquences du choix d'une contribution sur la modélisation des buts fonctionnels.

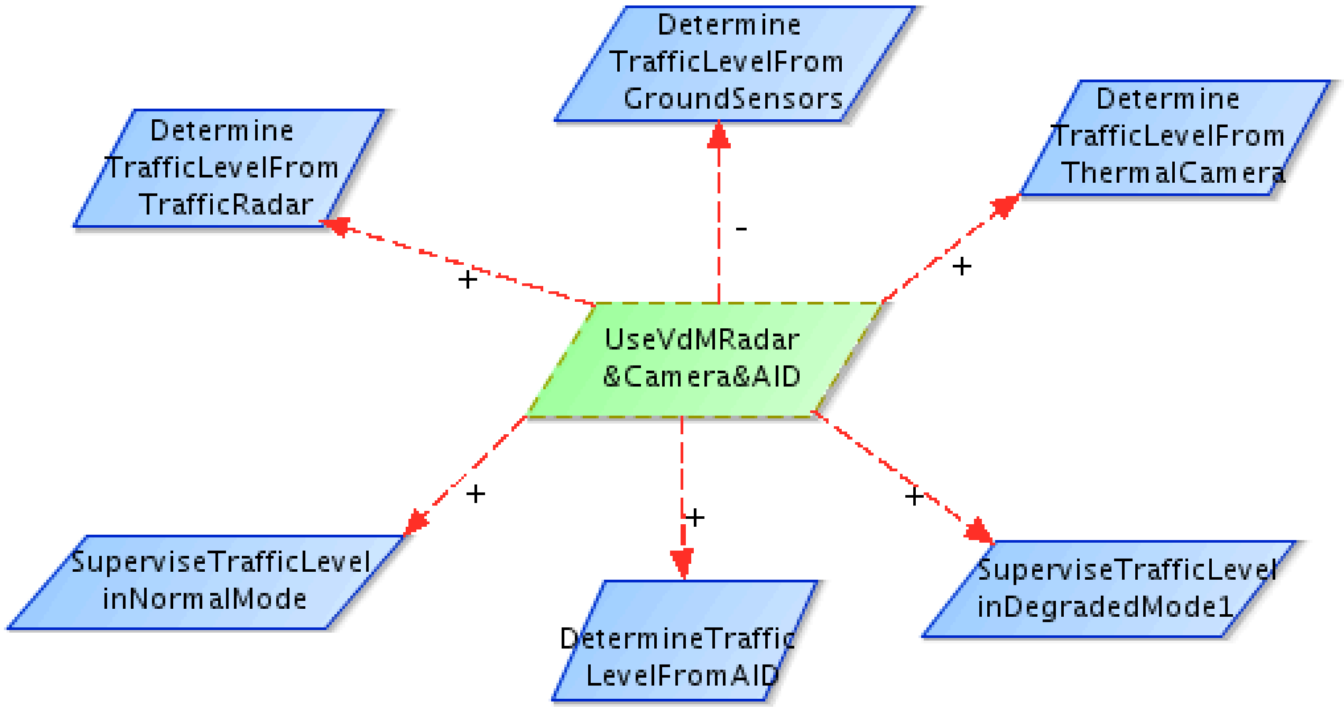

Figure 4 : Illustration de l'impact du non-fonctionnel sur le fonctionnel

Comme le montre la Figure 4, le choix du but de contribution **UseVdMRadar&Camera&AID** impose que la détermination du niveau de trafic se fasse avec l'AID du MTQ et avec le radar et la caméra thermique de la VdM. Ce choix impose également que la régulation du trafic se fasse, par ordre décroissant de priorité, en mode normal, puis dégradé I. Par contre, le choix exclut que la détermination du niveau de trafic se fasse à travers des capteurs souterrains.

e) Justification des modes de fonctionnement dégradés : modélisation des obstacles

La modélisation des obstacles [10] permet d'analyser les comportements attendus du système lorsque des obstacles empêchent la satisfaction d'un ou plusieurs buts fonctionnels. Un obstacle est une obstruction à la satisfaction d'un but fonctionnel. Les obstacles peuvent être raffinés afin de préciser les causes qui les produisent : un obstacle peut être causé par une conjonction ou une disjonction d'obstacles plus précis. De nouveaux buts fonctionnels ou contremesures peuvent en conséquence être définis aux fins de prévention, de détection ou de mitigation, et ainsi garantir un comportement adéquat du système.

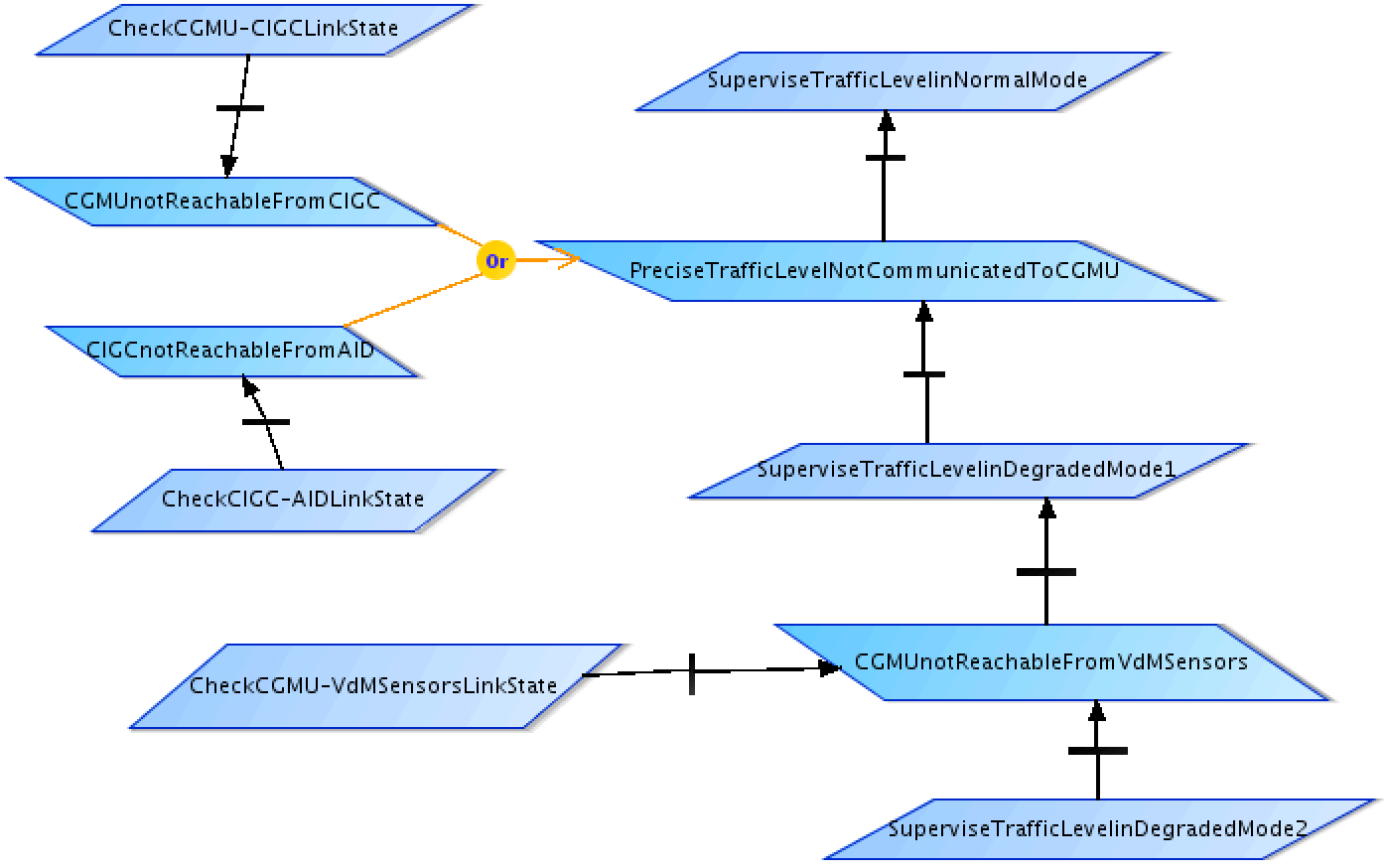

Figure 5: modélisation des obstacles (focus justification des modes dégradés)

La Figure 5 illustre la modélisation des obstacles ayant nécessité la mise en œuvre des modes de fonctionnement dégradés. La supervision du trafic en mode normal (but **SuperviseTrafficLevelinNormalMode** du modèle des buts fonctionnels [5]) peut être obstruée par l'impossibilité, pour l'AID, de faire parvenir une mesure précise de l'état du trafic au CGMU (obstacle **PreciseTrafficLevelNotCommunicatedToCGMU**). Cet obstacle peut être causé par l'indisponibilité du canal de communication entre le CGMU et le CIGC (obstacle **CGMUnotReachableFromCIGC**) ou par l'indisponibilité du canal de communication entre l'AID et le CIGC (obstacle **CIGCnotReachableFromAID**). Une contremesure permettant de détecter l'occurrence de l'obstacle **CGMUnotReachableFromCIGC** consiste à vérifier régulièrement l'état du canal de communication entre le CGMU et le CIGC (but fonctionnel **CheckCGMU-CIGCLinkState**). De même, le but fonctionnel **CheckCIGC-AIDLinkState** est proposé comme contremesure à l'obstacle **CIGCnotReachableFromAID**. Le but fonctionnel **SuperviseTrafficLevelinDegradedMode1**, défini dans le modèle des buts fonctionnels [5], permet un fonctionnement adéquat du système malgré l'obstacle **PreciseTrafficLevel-NotCommunicatedToCGMU**, en définissant une alternative permettant au CGMU de superviser le trafic sans passer par l'intermédiaire du CIGC**.** Toutefois, un obstacle à la satisfaction de **SuperviseTrafficLevelinDegradedMode1** est **CGMUnotReachableFromVdMSensors**, lié à l'impossibilité pour le CGMU de récupérer l'état du trafic estimé par les capteurs de la VdM positionnés à la sortie du tunnel. Face à cet obstacle, une contremesure de détection consiste à sonder régulièrement l'état du canal de communication entre le CGMU et les capteurs de la VdM (but fonctionnel **CheckCGMU-VdMSensorsLinkState**). Le but fonctionnel **SuperviseTrafficLevelinDegradedMode2** [5] est quant à lui défini comme contremesure de mitigation et consiste à envoyer un agent pour une supervision locale du trafic [8].

Discussion

La méthode SysML/KAOS permet globalement de bien modéliser les buts non fonctionnels et d'analyser les différentes façons de les satisfaire afin de justifier les choix effectués (à travers les buts de contribution). Toutefois, nous relevons les points suivants :

- Il serait intéressant et plus précis d'être en mesure de quantifier l'impact / la contribution d'un but, en plus de qualifier sa nature (positive/négative). Ceci pourrait se faire par exemple à l'aide de la notion de probabilité conditionnelle de satisfaction (-1 .. +1) : la probabilité que l'exigence non fonctionnelle soit satisfaite (ou pas) sachant que la contribution est sélectionnée ; le signe servant à qualifier la contribution/impact.
- Il serait intéressant d'introduire une nouvelle façon de raffiner un but non fonctionnel qui se traduirait par : pour satisfaire au maximum le but non fonctionnel ***NFG***, il faut satisfaire au max ***NFG*** dans les conditions correspondantes au prédicat ***P1***, le satisfaire au max dans les conditions correspondantes au prédicat ***P2***, …, et le satisfaire au max dans les conditions correspondantes au prédicat ***Pn***. *Exemple :* pour satisfaire au max l'exigence de disponibilité de l'état du trafic ***Availability[TL]***, il faut satisfaire au max ***Availability[TL]*** lorsque le lien *AID-CIGC-CGMU* est fonctionnel (mode *normal*), il faut satisfaire au max ***Availability[TL]*** lorsque le lien *AID-CIGC-CGMU* n'est pas fonctionnel mais le lien *VdM_Sensors-CGMU* est fonctionnel (mode *dégradé I*) et il faut satisfaire au max ***Availability[TL]*** lorsque ni le lien *AID-CIGC-CGMU*, ni le lien *VdM_Sensors-CGMU* ne sont fonctionnels. Ainsi, la contribution ***UseVdMRadar&Camera&AID,*** qui consiste à utiliser alternativement et par ordre de priorité chacune des sources, apparaîtrait naturellement comme la plus appropriée car satisfaisant au max les sous-buts et donc le but de haut niveau.
- Il serait intéressant d'introduire la possibilité de pouvoir raffiner des buts de contribution afin de :
    - Préciser le but de contribution ou le rendre moins abstrait pour par exemple le rendre plus digeste lors de la validation du modèle par les parties prenantes.
    - Faire apparaître des sous buts de contribution ayant des impacts ou des contributions spécifiques se généralisant à d'autres buts de contribution plus abstraits (buts parents) ou moins abstraits (buts enfants). Par exemple, les contributions liées à l'utilisation des capteurs de la VdM apparaîtraient au niveau d'un but de contribution abstrait (***useVdMSensors***) et les contributions spécifiques à l'utilisation du radar ou de la caméra thermique apparaîtraient au niveau des sous buts de contribution (***useRadar*** & ***useThermalCamera***) raffinant ***useVdMSensors***.
- Il serait intéressant d'introduire la modélisation des obstacles comme partie intégrante de SysML/KAOS et de distinguer les contremesures servant à détecter l'occurrence d'un obstacle de celles servant à le contourner. Par exemple, la contremesure **CheckCGMU-CIGCLinkState** se distinguerait de la contremesure **SuperviseTrafficLevelinDegradedMode1**. L'identification des obstacles et la génération des buts fonctionnels de contremesure pourrait se faire de façon systématique au sein du modèle des buts fonctionnels et on pourrait vérifier formellement que tous les obstacles sont couverts en se rassurant par exemple que des buts fonctionnels existent tels que la conjonction de leurs gardes correspond à la négation de la garde du but fonctionnel considéré.

Références

[1] S. J. Tueno Fotso, M. Frappier, R. Laleau et A. Mammar, «Modeling the hybrid ERTMS/ETCS level 3 standard using a formal requirements engineering approach,» *Lecture Notes in Computer Science,* vol. 10817, n° %1Abstract State Machines, Alloy, B, TLA, VDM, and Z - 6th International Conference, pp. 262-276, 2018.

[2] C. Gnaho, R. Laleau, F. Semmak et J.-M. Bruel, bCMS requirements modelling using SysML/KAOS.

[3] L. Chung, B. Nixon, E. Yu et J. Mylopoulos, Non-functional requirements in software engineering, Springer Science & Business Media, 2012.

[4] L. Chung, «Non-Functional Requirements,» The University of Texas at Dallas, Dallas, 2012.

[5] S. J. Tueno Fotso, «Projet Bonaventure Livrable 1 : modèle des buts fonctionnels,» Université de Sherbrooke, Sherbrooke, 2018.

[6] S. J. T. FOTSO, «Compte rendu réunion de kick-off du projet Bonaventure,» Sherbrooke, 2018.

[7] S. J. Tueno Fotso, «Compte rendu de la Séance de travail relative au projet Bonaventure du 26/09/2018,» Université de Sherbrooke, Sherbrooke, 2018.

[8] S. J. Tueno Fotso, «Compte rendu Séance de travail relative au projet Bonaventure du 22/11/2018,» Université de Sherbrooke, Sherbrooke, 2018.

[9] SMi, LES CONSULTANTS S.M. INC., «Annexe 4 -(Rapport APD) – Raccordement des rues Duke et de Nazareth à l'autoroute Ville-Marie,» Montréal, 2015.

[10] A. V. Lamsweerde, Specifications), Systematic Requirements Engineering (From System Goals to UML Models to Software, Wiley, 2008.

[11] Télécommunications GRIMARD, Entrepreneur spécialisé, «Système de détection d'évènement automatisé (DAI),» Laval, 2018.

[12] SMi, LES CONSULTANTS S.M. INC., «Raccordement des rues Duke et de Nazareth à l'autoroute Ville-Marie Avant-projet définitif,» Montréal, 2014.