

Projet Bonaventure

Livrable 2 : modèle des buts non-fonctionnels

Table des matières

| | |
|--|-----------|
| I- Description de la méthodologie | 1 |
| II- Modélisation des buts non-fonctionnels..... | 2 |
| 1- Cas du système de plus haut niveau | 3 |
| a) Identification des buts non-fonctionnels | 3 |
| b) Identification des buts de contribution..... | 5 |
| c) Illustration du diagramme des buts non-fonctionnels..... | 9 |
| d) Impact des buts non-fonctionnels sur les buts fonctionnels..... | 10 |
| Références..... | 11 |

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, efficacité, 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 l'étude réalisée par [2] et sur les taxonomies proposées dans [3] [4]. Elle se focalise sur la contrainte non fonctionnelle de sécurité **éviter les collisions dues à la courbure du tunnel** qui se traduit par des exigences 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'utilisateur : 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 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. La Figure 1 présente un extrait de la hiérarchisation des types de buts non-fonctionnels qui composent la contrainte de sécurité [3]. Ainsi, pour garantir la sécurité d'un système, il est nécessaire de garantir la disponibilité, l'intégrité et la confidentialité ; et, l'intégrité passe par la complétude et la précision. 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).

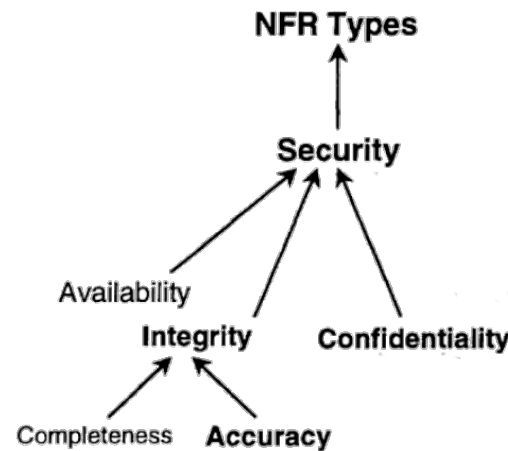


Figure 1: Extrait de la taxonomie des types de buts non-fonctionnels (focus buts de sécurité) [3]

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 négativement à la satisfaction d'un but non-fonctionnel élémentaire. 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- Cas du système de plus haut niveau

a) Identification des buts non-fonctionnels

| Niveau de raffinement | Identification du but | Description |
|-----------------------|--------------------------|--|
| 0 (niveau racine) | <i>Security [System]</i> | Contrainte de sécurité de plus haut niveau « éviter les collisions dues à la courbure du tunnel ». 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'utilisateur (état de la circulation et comportements recommandés) [5]. L'hypothèse sous-jacente est que l'utilisateur se conformera à la signalétique et aux recommandations qui lui sont adressées. |
| 1 | <i>Integrity [System]</i> | Garantir l'intégrité des données permettant de contrôler la signalisation routière à la sortie du tunnel et de notifier l'utilisateur [5]. |
| | <i>Availability [System]</i> | Garantir la disponibilité des données et modules permettant de contrôler la signalisation routière à la sortie du tunnel et de notifier l'utilisateur [5]. |
| 2 | <i>Integrity [TrafficSignalProgram]</i> | Garantir l'intégrité du plan de feux [6]. |
| | <i>Integrity [UserNotification]</i> | Garantir l'intégrité des notifications adressées aux usagers [6]. |
| | <i>Availability [TrafficLevel]</i> | Garantir la disponibilité des données de trafic [6]. |
| | <i>Availability [TrafficSignalProgram]</i> | Garantir la disponibilité du plan de feux et sa mise en œuvre [6]. |
| | <i>Availability [UserNotification]</i> | Garantir la disponibilité des notifications à adresser aux usagers et assurer leur diffusion [6]. |
| 3 | <i>Integrity [TrafficLevel-TSP]</i> | Garantir l'intégrité des données de trafic servant à déterminer le plan de feux [7]. |
| | <i>Integrity [CommunicatedTSP]</i> | Garantir l'intégrité du plan de feux reçu et appliqué au niveau des feux de signalisation [7]. |
| | <i>Integrity [TrafficLevel-UN]</i> | Garantir l'intégrité des données de trafic servant à déterminer les notifications à adresser aux usagers [7]. 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 <i>Integrity [TrafficLevel-TSP]</i> . |
| | <i>Integrity [CommunicatedUN]</i> | Garantir l'intégrité des notifications reçues par les usagers [6]. |
| | <i>Availability [Sensor]</i> | Garantir la disponibilité des capteurs permettant de détecter l'état du trafic [5] [6] [8]. Ce but dépend de la maintenabilité, de la réutilisabilité et, plus globalement, du coût de revient des capteurs sélectionnés. Le choix des capteurs au sol comme moyen de détection du niveau de trafic contribue par conséquent négativement à sa satisfaction. |
| | <i>Availability [PowerSupply]</i> | Garantir que chaque capteur utilisé ait accès à une source d'énergie adéquate [7]. |
| | <i>Availability [TSPController]</i> | Garantir la disponibilité d'un module (automate mécatronique, logiciel, etc.) capable de déterminer le plan de feux le plus adapté à l'état courant du trafic [6]. |
| | <i>Availability [TrafficLevel-TSPController]</i> | Garantir la disponibilité des données de trafic auprès du contrôleur chargé de déterminer le plan de feux [6]. |
| | <i>Availability [TrafficLight]</i> | Garantir la disponibilité des feux de signalisation [7]. Il s'agit ici d'assurer que si le plan de feu est correctement déterminé, les feux de signalisation l'appliqueront de façon à fournir les signaux adéquats aux usagers. |

| | | |
|---|---|---|
| | <i>Availability [DisplayInterface]</i> | Garantir la disponibilité des interfaces permettant de notifier les usagers (PMVs, équipements intelligents, etc.) [6]. |
| | <i>Availability [NotificationController]</i> | 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 [6]. |
| | <i>Availability [TrafficLevel-NotificationController]</i> | Garantir la disponibilité des données de trafic auprès du contrôleur chargé de déterminer les notifications à adresser aux usagers [6]. |
| 4 | <i>Accuracy [TrafficLevel-TSP]</i> | Garantir la précision des données de trafic servant à déterminer le plan de feux [7]. |
| | <i>Completeness [TrafficLevel-TSP]</i> | Garantir la complétude des données de trafic servant à déterminer le plan de feux [7]. |
| | <i>Accuracy [CommunicatedUN]</i> | Garantir la précision des notifications reçues par les usagers [6]. |
| | <i>Completeness [CommunicatedUN]</i> | Garantir que les notifications adressées aux usagers soient suffisamment riches pour qu'en s'y référant, il puisse sortir du tunnel en sécurité [6]. |
| | <i>Accuracy [TrafficLevel-UN]</i> | Garantir la précision des données de trafic servant à déterminer les notifications à adresser aux usagers [7]. Il est à préciser que ce but ne figure pas dans la représentation de la hiérarchie des buts pour des raisons de clarté. |
| | <i>Completeness [TrafficLevel-TSP]</i> | Garantir la complétude des données de trafic servant à déterminer les notifications à adresser aux usagers [7]. 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 déterminer le plan de feux et les notifications à l'attention des usagers. Ceci revient à se limiter au mode de fonctionnement normal uniquement. | <ul style="list-style-type: none"> Accuracy [TrafficLevel-TSP] Completeness [TrafficLevel-TSP] Accuracy [TrafficLevel-UN] Completeness [TrafficLevel-UN] Availability [Sensor] | <ul style="list-style-type: none"> Availability [TrafficLevel-TSPController] (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) |

| | | | |
|------------------------|--|--|---|
| | | | <ul style="list-style-type: none"> • Availability [TrafficLevel-NotificationController] |
| UseVdMCamera | Utiliser uniquement la caméra thermique de la VdM pour la détection du niveau de trafic. | <ul style="list-style-type: none"> • Availability [Sensor] | <ul style="list-style-type: none"> • Accuracy [TrafficLevel-TSP] (<i>l'usage des capteurs de la VdM ne permet pas d'atteindre le niveau de précision optimal (celui de l'AID))</i>) • Completeness [TrafficLevel-TSP] (<i>en utilisant uniquement la caméra thermique de la VdM, l'information obtenue n'est pas complète ; c'est pour ça que la VdM a combiné la caméra et le radar</i>) • Accuracy [TrafficLevel-UN] • Completeness [TrafficLevel-UN] • Availability [TrafficLevel-TSPController] (<i>car l'information de détection devra être transmise au CGMU alors que la liaison capteurs-CGMU n'est pas sûre</i>) • Availability [TrafficLevel-NotificationController] |
| UseVdMRadar | Utiliser uniquement le radar de trafic de la VdM pour la détection du niveau de trafic. | <ul style="list-style-type: none"> • Availability [Sensor] | <ul style="list-style-type: none"> • Accuracy [TrafficLevel-TSP] • Completeness [TrafficLevel-TSP] • Accuracy [TrafficLevel-UN] • Completeness [TrafficLevel-UN] • Availability [TrafficLevel-TSPController] • Availability [TrafficLevel-NotificationController] |
| 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 sera supprimé | <ul style="list-style-type: none"> • Accuracy [TrafficLevel-TSP] • Completeness [TrafficLevel-TSP] • Accuracy [TrafficLevel-UN] • Completeness [TrafficLevel-UN] • Availability [TrafficLevel-TSPController] |

| | | | |
|--|--|---|--|
| | | du modèle des buts non-fonctionnels. | <ul style="list-style-type: none"> • Availability [TrafficLevel-NotificationController] • Availability [Sensor] (<i>le capteur souterrain est difficilement maintenable et réutilisable, ce qui contribue négativement à la satisfiabilité de la contrainte de disponibilité des capteurs : par exemple, en cas de panne, il est très probable qu'il ne soit ni dépanné ni remplacé</i>) |
| UseVdMRadar & Camera-DG1 | 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 au mode de fonctionnement dégradé I uniquement. Le CGMU est la seule entité responsable de la détermination du plan de feux. | <ul style="list-style-type: none"> • Completeness [TrafficLevel-TSP] • Completeness [TrafficLevel-UN] • Availability [Sensor] | <ul style="list-style-type: none"> • Availability [TrafficLevel-TSPController] • Availability [TrafficLevel-NotificationController] • Accuracy [TrafficLevel-TSP] • Accuracy [TrafficLevel-UN] |
| UseVdMRadar & Camera-DG2 | Combiner la caméra thermique et le radar de trafic de la VdM pour détecter le niveau de trafic à transmettre à l'automate de contrôle de trafic. Ceci revient à se limiter au mode de fonctionnement dégradé II uniquement. L'automate est la seule entité responsable de la détermination du plan de feux. | <ul style="list-style-type: none"> • Completeness [TrafficLevel-TSP] • Completeness [TrafficLevel-UN] • Availability [Sensor] • Availability [TrafficLevel-TSPController] | <ul style="list-style-type: none"> • Accuracy [TrafficLevel-TSP] • Accuracy [TrafficLevel-UN] • Integrity [CommunicatedTSP] (<i>l'automate choisi entre des plans préétablis et très stricts</i>) • Availability [TrafficLevel-NotificationController] • Availability [NotificationController] (<i>l'automate ne contrôle pas l'envoi des notifications aux utilisateurs</i>) |
| UseAlternatively-AID-VdM Radar&Camera-DG1&DG2 | Utiliser alternativement les modes de fonctionnement normal (utilisation de l'AID), dégradé I (utilisation des capteurs du CGMU avec le CGMU pour déterminer les plans de feux) et dégradé II (utilisation | <ul style="list-style-type: none"> • Completeness [TrafficLevel-TSP] • Completeness [TrafficLevel-UN] • Accuracy [TrafficLevel-TSP] • Accuracy [TrafficLevel-UN] | |

| | | | |
|-----------------|--|--|--|
| | des capteurs du CGMU avec l'automate de contrôle de trafic pour déterminer les plans de feux). Il est à préciser que ce but ne figure pas dans la représentation de la hiérarchie des buts pour des raisons de clarté. | <ul style="list-style-type: none"> • Availability [TrafficLevel-NotificationController] • Availability [TrafficLevel-TSPController] • Availability [Sensor] | |
| UsePMV | Utiliser les panneaux à message variable pour la notification des usagers. | <ul style="list-style-type: none"> • Accuracy [CommunicatedUN] • Availability [DisplayInterface] | <ul style="list-style-type: none"> • Completeness [CommunicatedUN] |
| UseWaze | Utiliser la plateforme Waze pour la notification des usagers. | <ul style="list-style-type: none"> • Accuracy [CommunicatedUN] • Completeness [CommunicatedUN] | <ul style="list-style-type: none"> • Availability [DisplayInterface] (<i>impossible de garantir que l'utilisateur aura le client Waze</i>) |
| UseGMaps | Utiliser la plateforme Google Maps pour la notification des usagers. | <ul style="list-style-type: none"> • Accuracy [CommunicatedUN] • Completeness [CommunicatedUN] | <ul style="list-style-type: none"> • Availability [DisplayInterface] (<i>impossible de garantir que l'utilisateur aura le client GMaps</i>) |

c) Illustration du diagramme des buts non-fonctionnels

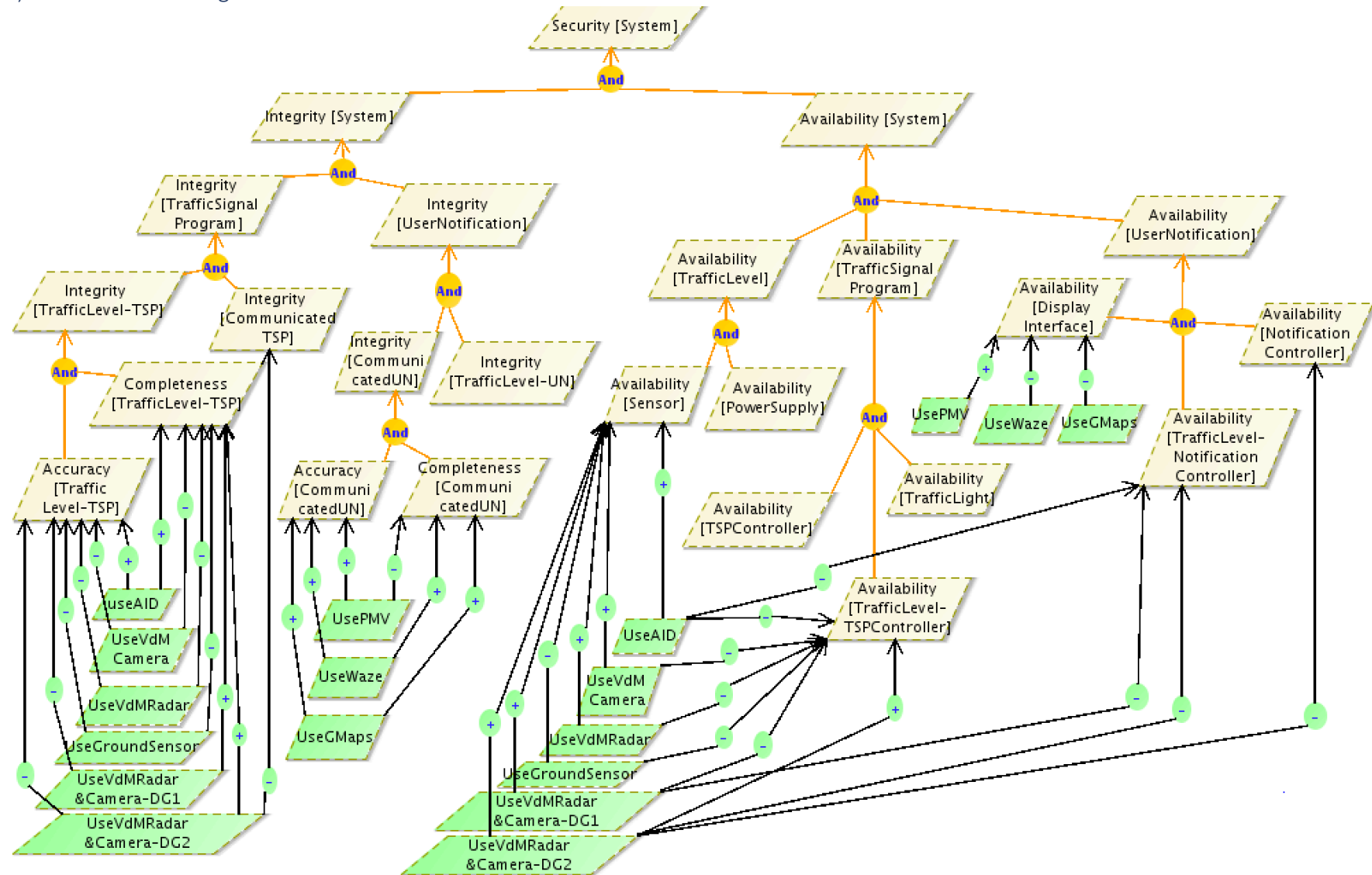


Figure 2: Diagramme des buts non-fonctionnels du système principal

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

Pour cette partie, nous nous limitons au but de contribution **UseAlternatively-AID-VdMRadar&Camera-DG1&DG2** 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.

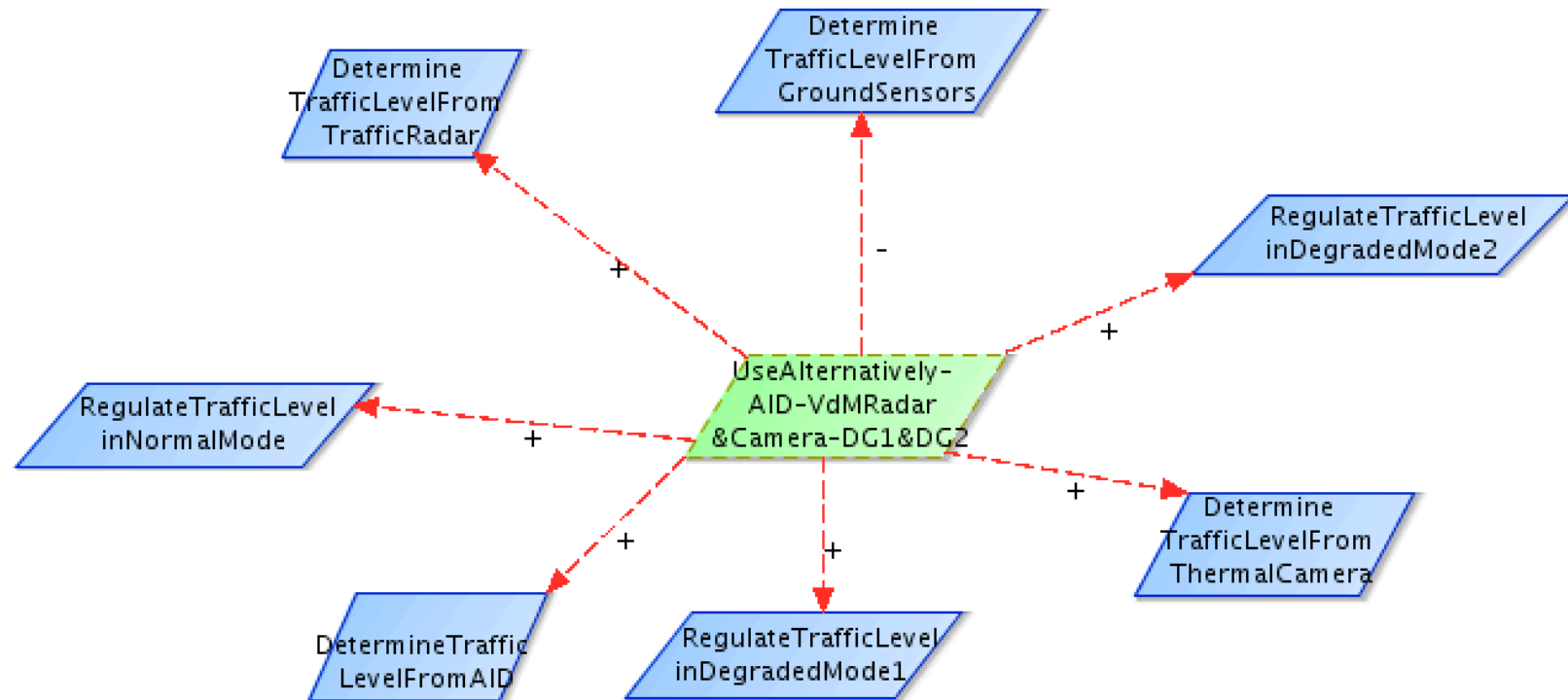


Figure 3 : Illustration de l'impact du non-fonctionnel sur le fonctionnel

Comme le montre la Figure 3, le choix du but de contribution **UseAlternatively-AID-VdMRadar&Camera-DG1&DG2** 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, dégradé I et dégradé II. Par contre, le choix exclut que la détermination du niveau de trafic se fasse à travers des capteurs au sol.

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° 1 Abstract 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. T. FOTSO, «Compte rendu réunion de kick-off du projet Bonaventure,» Sherbrooke, 2018.
- [6] S. J. Tueno Fotso, «Compte rendu de la Séance de travail relative au projet Bonaventure du 26/09/2018,» Université de Sherbrooke, Sherbrooke, 2018.
- [7] SMi, LES CONSULTANTS S.M. INC., «Annexe 4 -(Rapport APD) – Raccordement des rues Duke et de Nazareth à l'autoroute Ville-Marie,» Montréal, 2015.
- [8] Télécommunications GRIMARD, Entrepreneur spécialisé, «Système de détection d'évènement automatisé (DAI),» Laval, 2018.
- [9] SMi, LES CONSULTANTS S.M. INC., «Raccordement des rues Duke et de Nazareth à l'autoroute Ville-Marie Avant-projet définitif,» Montréal, 2014.