ANR programme ARPEGE 2008

Systèmes Embarqués et Grandes Infrastructures

Projet SELKIS : Une méthode de développement de systèmes d'information médicaux sécurisés : de l'analyse des besoins à l'implémentation.

ANR-08-SEGI-018

Février 2009 - Décembre 2011

Analysis of security requirements for Res@mu - Analyse des besoins de sécurité pour Res@mu

Livrable numero 6.1.1

Akram Idani, LIG
Mohamed-Amine Labiadh, LIG
Yves Ledru, LIG
Jean-Luc Richier, LIG
Quentin Switsers, IFREMMONT
Pascal Zellner, IFREMMONT

2 mars 2010

Table des matières

Chapitre 1

Introduction

Ce document présente l'analyse des besoins de sécurité de l'étude de cas Res@mu proposée par IFREMMONT dans le cadre du projet Selkis.

Ce document comprend 4 parties :

- Chapitre 2 : Un modèle fonctionnel de l'application Res@mu : ce modèle fonctionnel présente la structuration des données dans des diagrammes de classes et l'identification de use cases. Le modèle fonctionnel a été établi avant l'analyse des besoins de sécurité.
- Chapitre 3 : Une étude préliminaire des besoins de sécurité qui a identifié les principaux agents du système et les principales propriétés de sécurité.
- Chapitre 4 : La présentation de la méthode suivie pour mettre en relation les propriétés de sécurité de haut niveau, les buts fonctionnels et les règles de contrôle d'accès qui mettent en oeuvre cette politique de sécurité.
- Chapitre 5 : Le résultat de l'application de cette méthode.

La modélisation fonctionnelle a été préparée par IFREMMONT. Le modèle de buts et les règles RBAC ont été préparées par le LIG. Deux réunions ont contribué à la compréhension mutuelle entre les équipes et à la validation de ces modèles.

CHAPITRE 2 : MODELISATION FONCTIONNELLE

INTRODUCTION

DESCRIPTION DU DOCUMENT

Ce document a pour but de décrire de façon détaillée le contexte dans lequel opère le projet Selkis, appliqué au projet de SI préhospitalier, héritier du projet Res@mu. Validé par des experts métier, il sert de document de référence à la suite du projet, tant dans la terminologie que dans les fonctionnalités.

LE PROJET SELKIS APPLIQUE AU RES@MU

Le projet Selkis vise à redéfinir les flux et les formats d'échanges des informations transmises par le SI préhospitalier, qui bénéficiera ainsi des avancées proposées par la méthodologie SELKIS.

LE MILIEU PRE-HOSPITALIER

Le futur SI couvre le périmètre pré-hospitalier, c'est-à-dire en dehors du cadre hospitalier, en amont et/ou en aval d'une éventuelle hospitalisation. Il s'agit donc d'interventions en extérieur, où les professionnels de santé se déplacent en fonction du patient, que ce soient des interventions d'urgence (suite à un appel au centre 15 ou au 18), des interventions d'hospitalisation à domicile, des futurs centres d'aide médicale à la personne…

L'ORGANISATION DES MOYENS

LES UNITES

Tout moyen, qu'il soit matériel ou humain, appartient à une et une seule unité (à un instant donné, un moyen pouvant changer d'unité au cours du temps), l'unité est la structure médicale, on y distingue par exemple les sapeurs pompiers, le SAMU, le SMUR, les équipes d'HAD, etc.

Les unités sont présentes sur différentes bases opérationnelles. On définit comme base opérationnelle une structure immobilière, telle qu'un centre hospitalier, une caserne, etc. qui accueille une et une seule unité. Si plusieurs unités sont présentes dans une même structure immobilière, on distinguera tout de même autant de bases opérationnelles qu'il y a d'unités.

On distingue trois types d'unités, d'où trois types de bases opérationnelles :

- les unités de régulation, installées dans des centres de régulation ;
- les unités mobiles de soin, installées dans des centres de secours ;
- les unités d'accueil, installées dans des centres de soins.

Les unités mobiles de soin et les unités d'accueil sont désignées comme des unités médicales, et leurs bases opérationnelles comme centres médicaux.

LES UNITES DE REGULATION

Les unités de régulation sont les unités qui reçoivent les appels d'urgence, et organisent l'envoi des moyens des unités médicales. Elles peuvent également servir de relais aux équipes en intervention qui réclament de l'aide, soit en effectifs sur place, soit en avis médicaux particuliers. Les centres de régulation actuellement pris en compte sont :

- le SAMU (15) ;
- le SDIS ;
- les Sapeurs-Pompiers (18) ;
- Les centres de gestion de services d'aide à la personne.

LES UNITES MOBILES DE SOINS

Les unités mobiles de soins sont les unités dont le personnel est envoyé sur le lieu des interventions. Les unités mobiles de soins actuellement prises en compte sont :

- le SMUR ;
- les Sapeur Pompiers ;
- les compagnies d'ambulances privées ;
- les unités d'hospitalisation à domicile ;
- les organisations de secouristes ;
- le PGHM ;
- les CRS ;
- les secouristes du Spéléo Club Français.

À chaque centre de secours est affectée une liste de communes, sur lesquelles il est plus ou moins prioritaire suivant un certain niveau de priorité (allant de 1 à 3).

LES UNITES D'ACCUEIL

Les unités d'accueil (cf. figure 1) sont les unités pouvant accueillir des patients pour des soins ou des examens spécifiques, ou pour une hospitalisation prolongée. Les services d'accueil actuellement pris en compte sont :

- les services d'accueil des urgences ;
- les services de déchoquage ;
- les USIC ;
- les unités de réanimation polyvalente ;
- les unités de réanimation chirurgicale ;
- les unités de réanimation neuro-chirurgicale.

Le personnel des services d'accueil n'a pas vocation à se déplacer, mais il peut néanmoins être amené à se rendre sur le lieu d'interventions. Il intègre alors une équipe d'une unité mobile de soins.

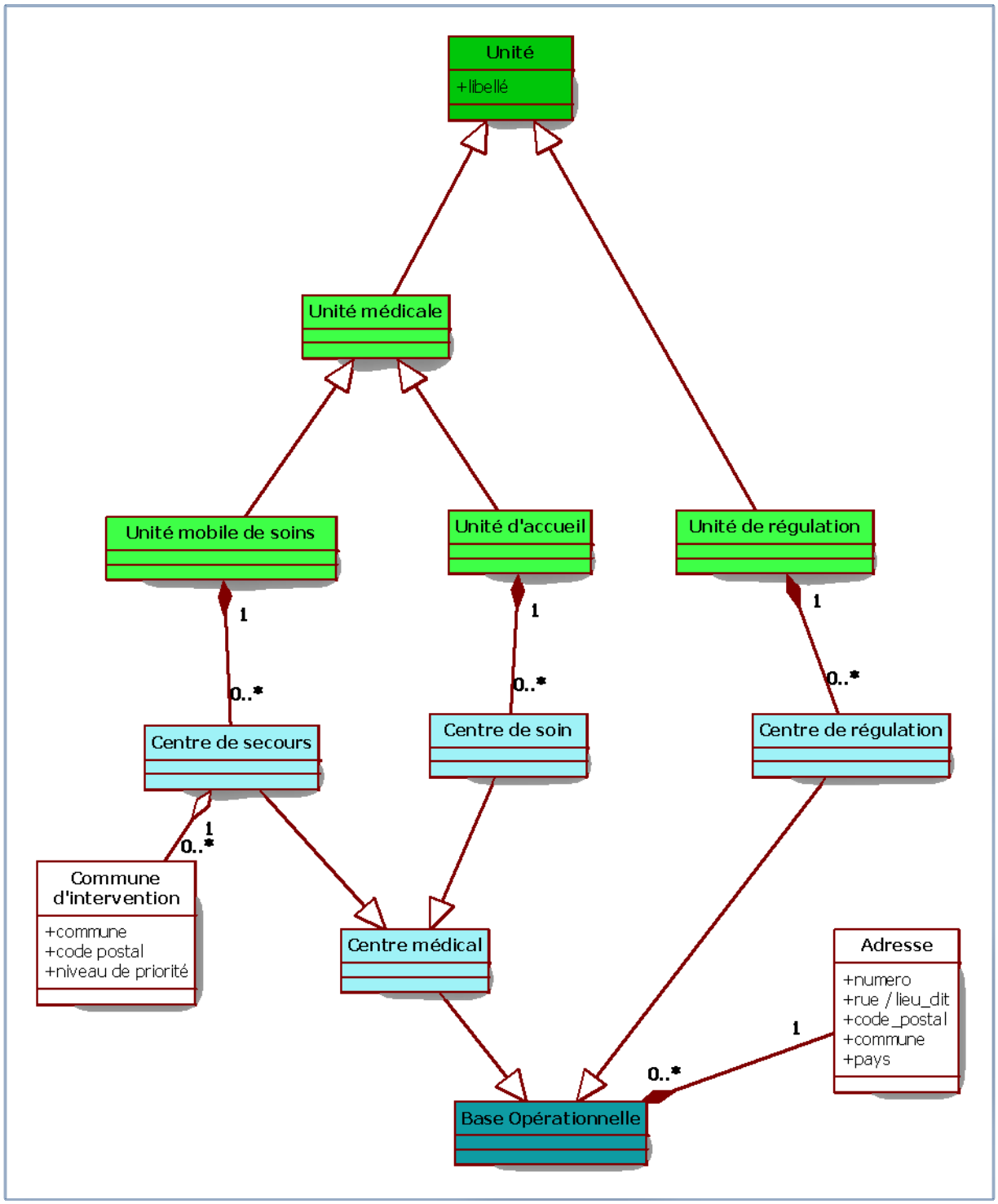


Figure 1 - Diagramme des unités

LES MOYENS HUMAINS

Pour chaque moyen humain (cf. figure 2) enregistré, on connait :

- son nom ;
- son prénom ;
- la base opérationnelle à laquelle il est rattaché ;
- sa ou ses fonctions ;
- ses droits administrateur au sein du SI pré hospitalier ;
- son numéro de téléphone.

On distingue deux grands types de fonctions :

- opérateur ;
- professionnel de santé.

LES OPERATEURS

Les opérateurs (cf. Figure 2) agissent au sein de leur base opérationnelle, et assurent l'organisation générale de leurs moyens et la communication avec les autres bases opérationnelles. Ils sont également en charge de la planification des interventions programmées.

On distingue pour chaque type d'unité un type d'opérateur:

- les opérateurs de régulation : ils répondent aux appels d'urgence, et font appel aux moyens nécessaires en conséquence. Ils peuvent également servir de relais aux demandes d'aide des équipes en intervention, que ce soit une demande d'envoi de moyen ou d'avis médical auprès d'un médecin spécialisé ;
- les opérateurs de centres médicaux (qui regroupent les opérateurs de centres de soin et de centres de secours) : ils répondent aux demandes d'aide qui leur sont transmises, et constituent les équipes en conséquence. Ils sont chargés du maintient à jour de la disponibilité des moyens de leur base opérationnelle. Les opérateurs de centres de secours gèrent par ailleurs les stocks en équipements médicaux et en matériels consommables de leur centre et des véhicules d'interventions qui y sont attachés.

LES PROFESSIONNELS DE SANTE

Les professionnels de santé (cf. Figure 3) sont les personnels amenés à prendre en charge des patients, sur place ou à distance.

On distingue quatre grands types de professionnels de santé :

- les infirmiers : ils appartiennent aux centres de secours, et font partie des équipes mobiles envoyées en intervention ;
- les secouristes : de même que les infirmiers, ils appartiennent aux centres de secours et font partie des équipes mobiles envoyées en intervention. On distingue parmi les secouristes les ambulanciers, habilités à conduire les véhicules d'intervention ;
- les médecins : on en trouve généralement au moins un par équipe. Ils sont responsables de la prise en charge des patients. On distingue parmi eux :

  - Δ les médecins régulateurs : ils appartiennent aux centres de régulation, et ne peuvent prendre en charge un patient qu'à distance ;
  - Δ les médecins fixes : ils appartiennent aux centres de soin. Ils sont en poste dans leur centre, mais peuvent être amenés à se déplacer sur le lieu d'une intervention. Ils peuvent également être appelés à fournir un avis médical à distance ;
  - Δ les médecins mobiles : ils appartiennent aux centres de secours, et interviennent le plus souvent directement sur le patient. Ils peuvent néanmoins également être appelés à fournir leur avis à distance.
- les opérateurs médicaux (PARM) : ils appartiennent aux centres de régulation, et sont habilités à fournir des conseils médicaux à distance.

Tout professionnel de santé est nécessairement dans l'un des états suivants :

- disponible à sa base opérationnelle, en attente d'intervention ;
- disponible hors de sa base opérationnelle (par exemple de retour d'une intervention) ;
- en intervention, donc indisponible ;
- indisponible, lorsqu'il n'est pas de garde ou pour d'autres motifs.

EQUIPES PRE-ETABLIES

Les professionnels de santé qui sont de garde et en attente à leur base opérationnelle peuvent être regroupés en équipes préétablies (Figure 4). Celles-ci permettent une visualisation simplifiée des moyens disponibles, mais n'engagent à rien concernant la constitution des équipes finalement envoyées en intervention.

Un professionnel de santé peut faire partie de plusieurs équipes préétablies, mais sitôt qu'un des membres de l'équipe n'est plus disponible, l'équipe préétablie n'existe plus.

Aux équipes préétablies peuvent également être associés un ou plusieurs véhicules d'intervention.

LES VEHICULES D'INTERVENTIONS

Le contexte pré-hospitalier comprend une flotte de véhicules (Figure 4) d'intervention. Chacun est plus ou moins adapté à intervenir dans des situations géographiques et sur des interventions particulières. Tout véhicule est rattaché à un centre de secours, où il est stationné lorsqu'il est inactif. Chaque véhicule peut par ailleurs être localisé instantanément par GPS.

Chaque véhicule est nécessairement dans l'un des états suivants :

- stationné à sa base opérationnelle, prêt à partir ;
- en intervention ;
- hors de sa base opérationnelle, mais disponible pour une intervention ;
- indisponible (en panne ou en maintenance).

Tous les véhicules possèdent une pharmacie, contenant du matériel médical consommable. Lorsqu'un véhicule part en intervention, cette pharmacie se doit d'être correctement fournie. Un inventaire précis et à jour de celle-ci est donc indispensable.

De même, chaque véhicule contient des équipements médicaux particuliers, qui peuvent être amenés à être changés. La mise à jour de ces équipements est donc également indispensable.

Chaque véhicule peut être joint par radio ou par téléphone.

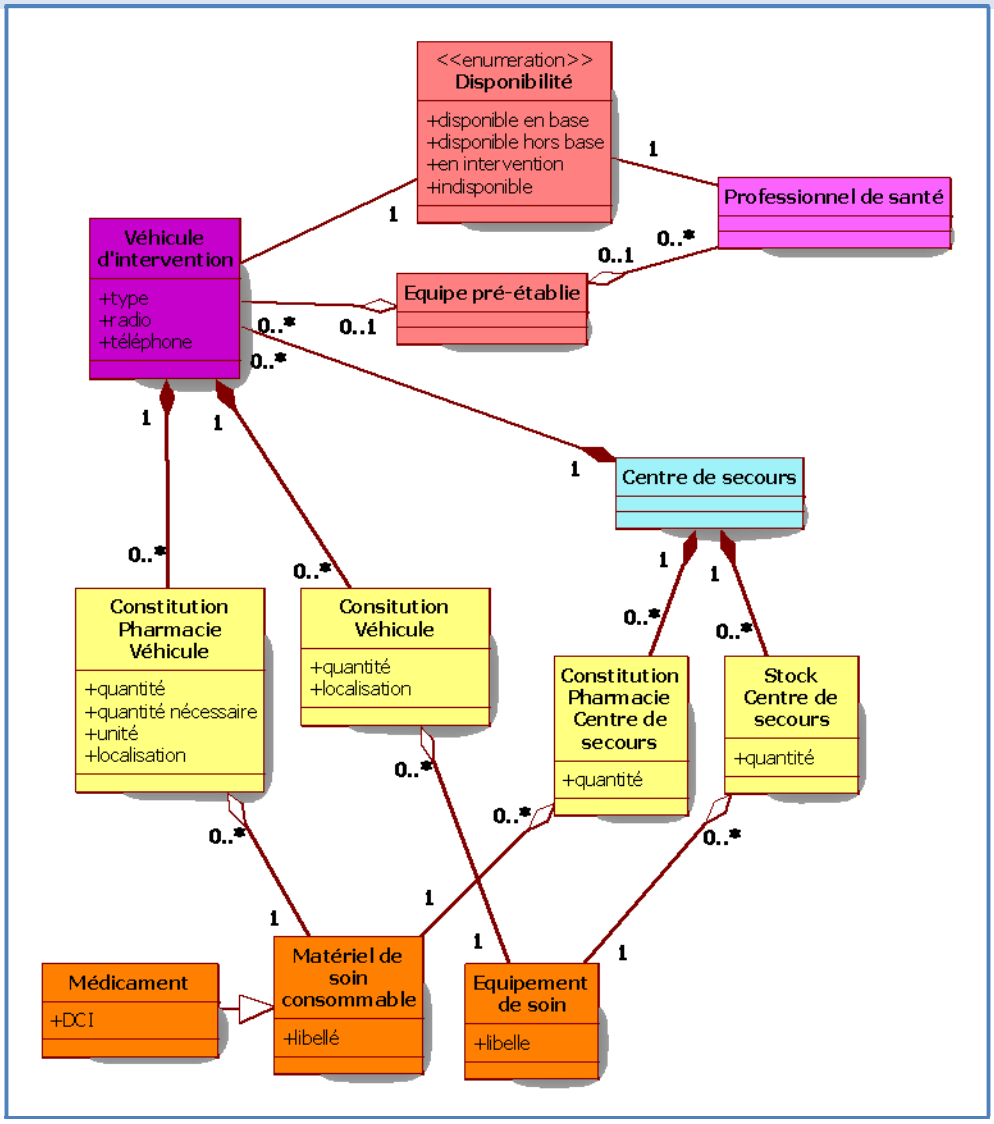


Figure 2 - Diagramme Véhicules

LES INTERVENTIONS

Chaque intervention implique la prise en charge d'un ou plusieurs patients. On distingue dans le contexte préhospitalier deux types d'interventions :

- les interventions de secours : elles ont lieu lors d'accidents à l'extérieur, et sont déclenchées par un appel à la régulation ;
- les interventions programmées : elles sont planifiées par le corps médical sur des patients hospitalisés à domicile (ou apparenté, comme par exemple en maison de retraite) ou en centre de soin (lorsque l'intervention nécessite le transport du patient vers un autre centre de soin).

Pour chaque intervention, on renseignera les informations suivantes (à choisir dans un thésaurus ou à renseigner en texte libre) :

- le motif de recours au soin ;
- les circonstances qui ont amené le patient à avoir recours au soin ;
- le type de lieu de l'intervention ;
- la localisation de l'intervention.

Seront également enregistrées les heures de début et de fin de l'intervention. Peuvent également être attachées à une intervention une ou plusieurs pièces jointes (plan d'évacuation, photographie…).

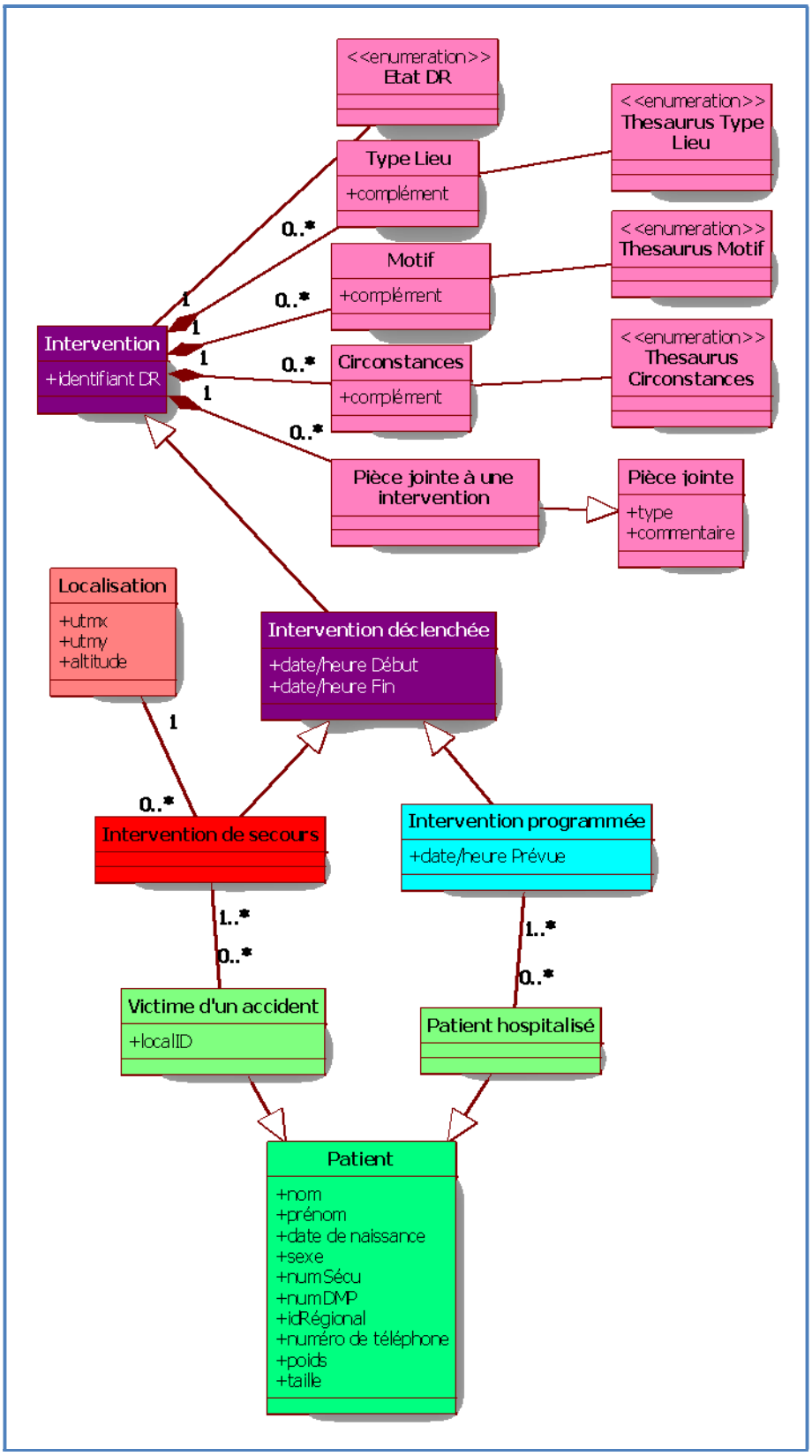


Figure 3 - Diagramme des interventions

ORGANISATION DES MOYENS

Tout professionnel de santé prenant part à une intervention appartient nécessairement à une équipe (même si elle n'est composée que d'un seul membre), formée pour l'occasion, et dissoute à la fin de l'intervention. Ces équipes sont généralement constituées de personnel d'une même unité, mais elles peuvent également être amenées à intégrer du personnel d'une autre unité.

Plusieurs équipes peuvent participer à une même intervention, en même temps ou en différé. Si une équipe fait appel à du renfort sur une intervention, elle le fait soit directement via l'unité concernée, soit via un centre de régulation qui relaye alors cet appel.

On distingue deux types d'équipes :

- les équipes mobiles : elles sont amenées à se déplacer, soit pour se rendre sur les lieux de l'intervention, soit pour transporter un patient. Elles sont en contact direct avec les patients. Elles appartiennent nécessairement à une unité mobile de soin (même si tous ces membres ne sont pas de cette unité). Elles sont généralement associées à un ou plusieurs véhicules d'interventions, qui peuvent changer au cours de l'intervention ;
- les équipes distantes : elles agissent à distance sur une intervention, et ne sont pas en contact direct avec les patients. Elles ne sont généralement composées que d'un membre, et aident les équipes sur place en donnant un avis médical.

La constitution d'une équipe est généralement fixe sur une intervention, mais elle peut être amenée à se diviser ou à intégrer des membres au cours d'une intervention. On considère que tous les membres d'une équipe sont à une même localisation et dans un même état.

Pour chaque équipe, on note :

- l'heure de création de l'équipe ;
- l'heure de fin de mission.

Concernant les équipes mobiles, on note également :

- l'heure de départ pour les lieux de l'intervention ;
- l'heure d'arrivée sur les lieux de l'intervention ;
- l'heure de départ des lieux de l'intervention.

De plus, chacun de ses déplacements sont enregistrés. Pour chaque étape, on note alors :

- la localisation de départ ;
- l'heure de départ ;
- la localisation d'arrivée ;
- l'heure d'arrivée ;
- le motif du déplacement.

Une équipe peut à tout moment interrompre sa participation à une intervention. Elle note alors l'heure et le motif de cette décision.

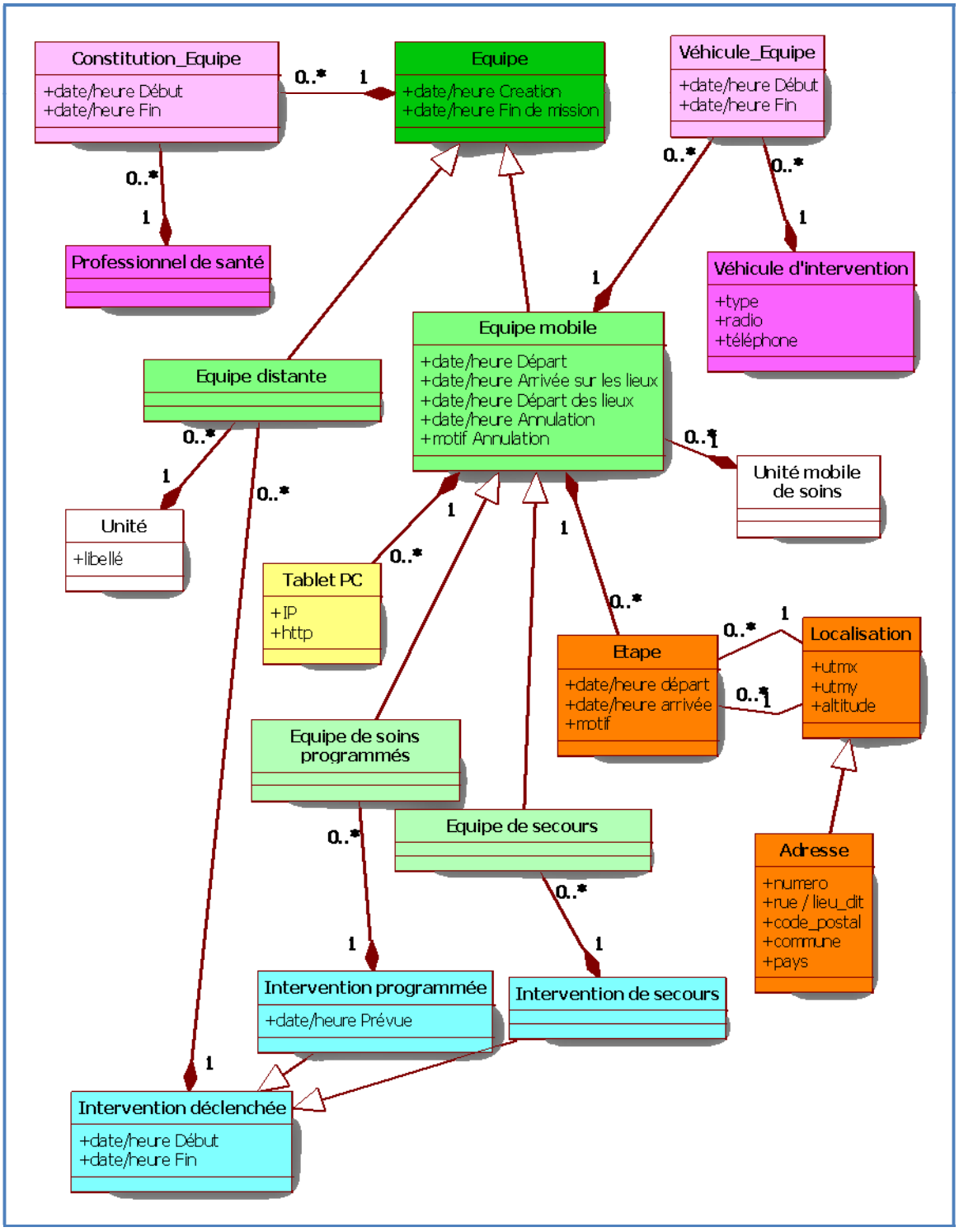


Figure 4 - Diagramme des équipes

REGULATION

TRAITEMENT DES APPELS D'URGENCE

Les appels d'urgence sont les appels de particuliers reçus par les unités de régulation lors d'accidents en extérieur. Chaque appel entraine la création d'un dossier de régulation, dans lequel seront notées toutes les informations relatives à cet appel et à son traitement par la régulation.

Pour chaque appel, on note :

- le nom de l'appelant ;
- le prénom ;
- le numéro de téléphone ;
- la provenance (privée, ou d'une structure particulière) ;
- le type de l'appelant (son lien avec l'intervention et le ou les patients).

Chaque étape de l'appel est horodatée. On enregistre donc l'heure de l'appel, puis les différents états d'un appel, à savoir :

- rejeté : l'appel est automatiquement rejeté, avant même d'être présenté à la régulation ;
- présenté : l'appel parvient à un centre de régulation, et attend d'être traité ;
- répondu : l'appel est pris en charge, soit par un opérateur de régulation, soit automatiquement via un serveur vocal interactif ;
- perdu : appel présenté mais raccroché par l'appelant avant d'être répondu ;
- raccroché : appel répondu raccroché.

Par ailleurs, un appel peut être transféré vers un autre opérateur, voire vers un autre centre de régulation. L'heure et le motif de ce transfert sont alors enregistrés.

Un ou plusieurs scores de priorité peuvent être attribués à un appel, suivant des normes propres à chaque unité de régulation.

Le ou les patients peuvent soit être pris en charge à distance par un médecin régulateur ou par un PARM, soit par des professionnels de santé d'une unité de soins mobile envoyés sur place. Dans ce second cas, l'opérateur de régulation visualise les moyens disponibles, et fait une demande d'aide aux centres de secours concernés.

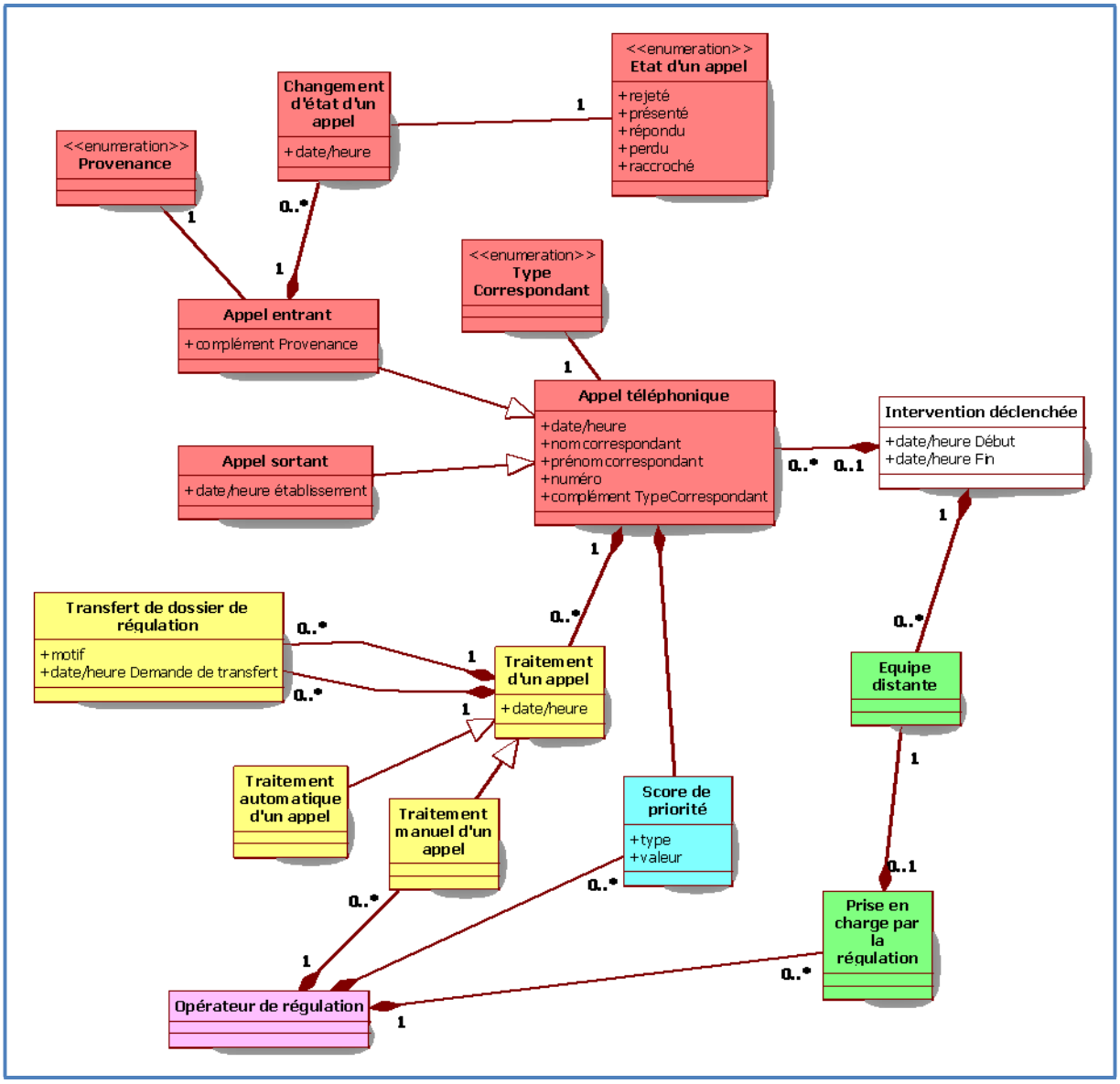


Figure 5 - Diagramme des appels

DEMANDE D'AIDE

Les demandes d'aide (Figure 9) sont adressées aux centres médicaux, soit par la régulation, soit par une équipe déjà en charge sur l'intervention. Une équipe peut également transmettre une demande d'aide à la régulation, qui la relaye aux centres médicaux concernés.

L'heure de la réception d'une demande d'aide ainsi que son motif sont notés. Le centre médical à qui elle a été adressée peut alors soit confirmer son aide (elle constitue ensuite la ou les équipes qui participent à l'intervention), soit la refuser (on note alors le motif de refus).

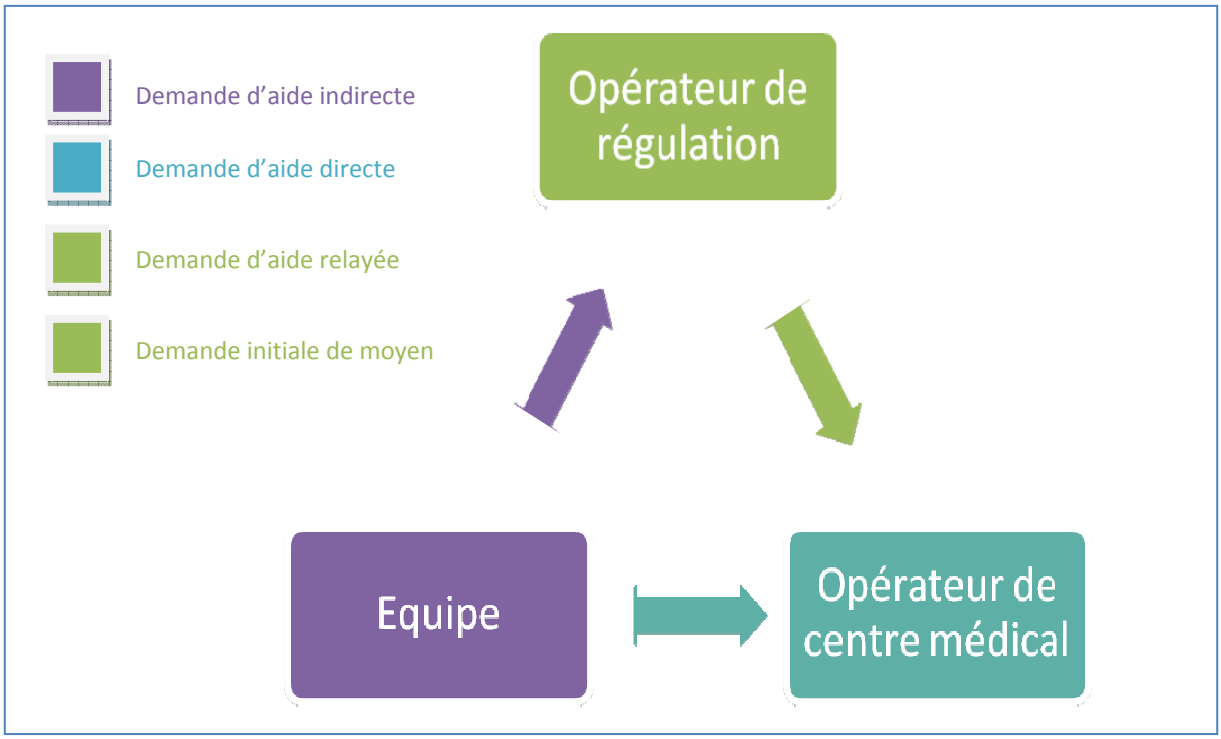


Figure 6 – Type de demande d'aide

- les demandes d'envoi de moyens : l'intervention nécessite que des moyens soient envoyés sur place ;
- les demandes d'avis médical : la prise en charge d'un patient nécessite l'avis d'un médecin spécialisé, auquel sont envoyées toutes les données du patient pour une prise en charge à distance.

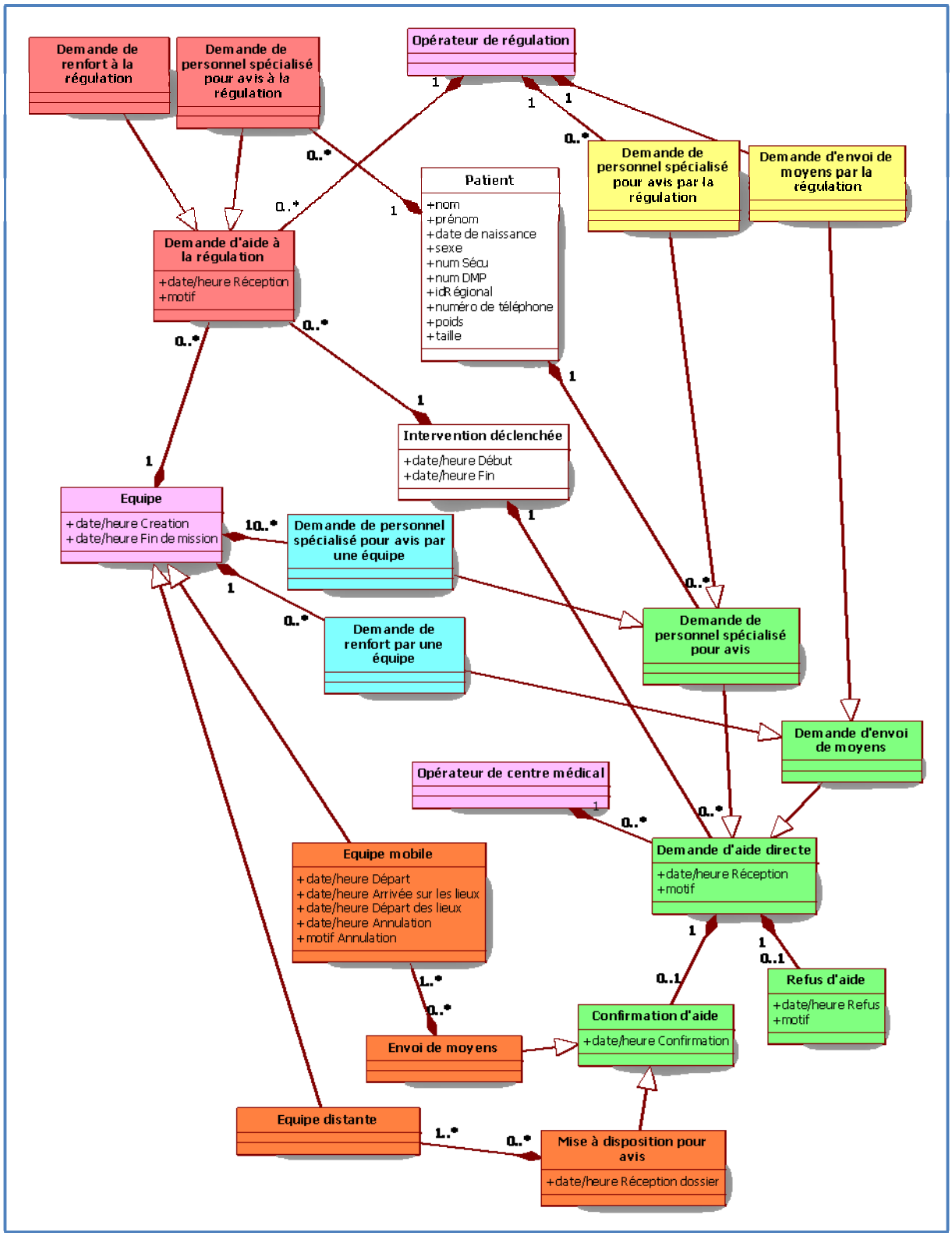


Figure 7 - Diagramme des demandes d'aide

DEMANDE DE PLACE D'ACCUEIL

Dans le cas où la prise en charge d'un patient nécessite l'accueil dans un centre de soin (examen, soin spécifique ou hospitalisation prolongée), une demande de place d'accueil est adressée à ce centre de soin. Cette demande peut être effectuée soit par un autre centre de soin, soit par une équipe en charge du patient. Elle peut être adressée soit directement au centre de soin concerné, soit à la régulation, qui relaye cette demande (Figure 10).

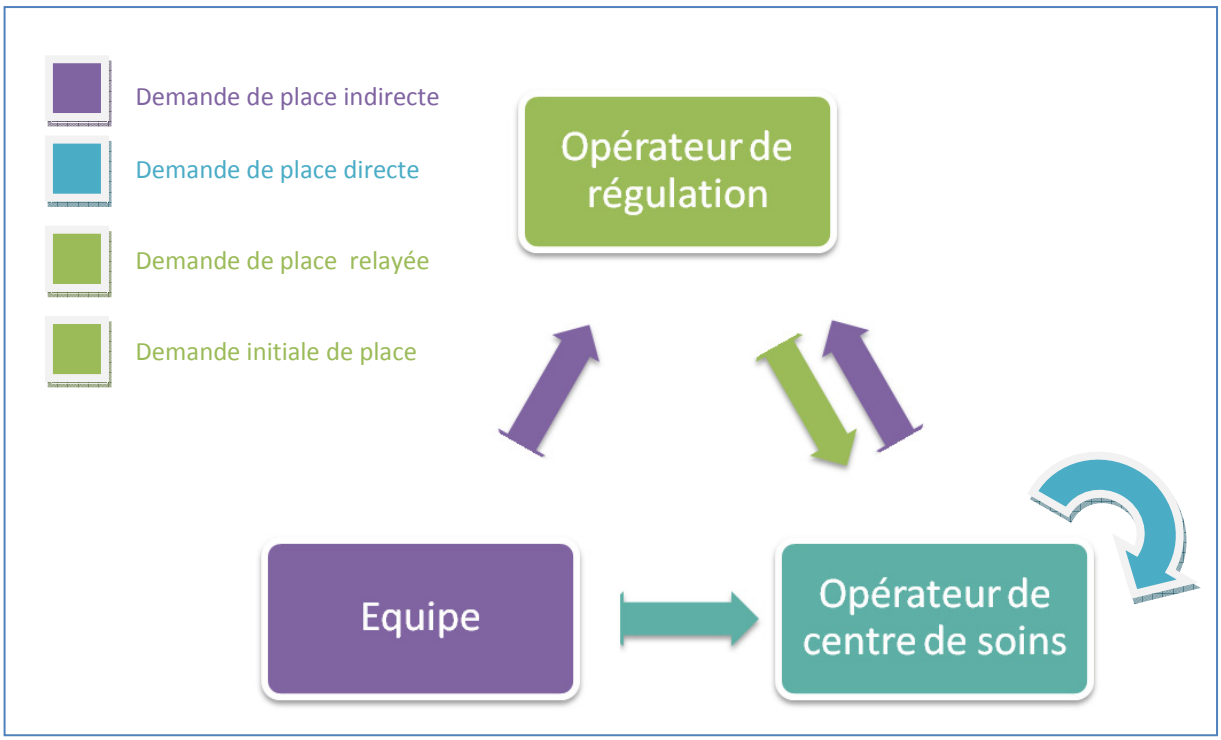


Figure 8 - Type de demande de place d'accueil

L'heure de la réception d'une demande de place d'accueil ainsi que son motif sont notés. Le centre de soin à qui elle a été adressée peut alors soit confirmer, soit refuser (Figure 11) l'accueil du patient dans ses locaux.

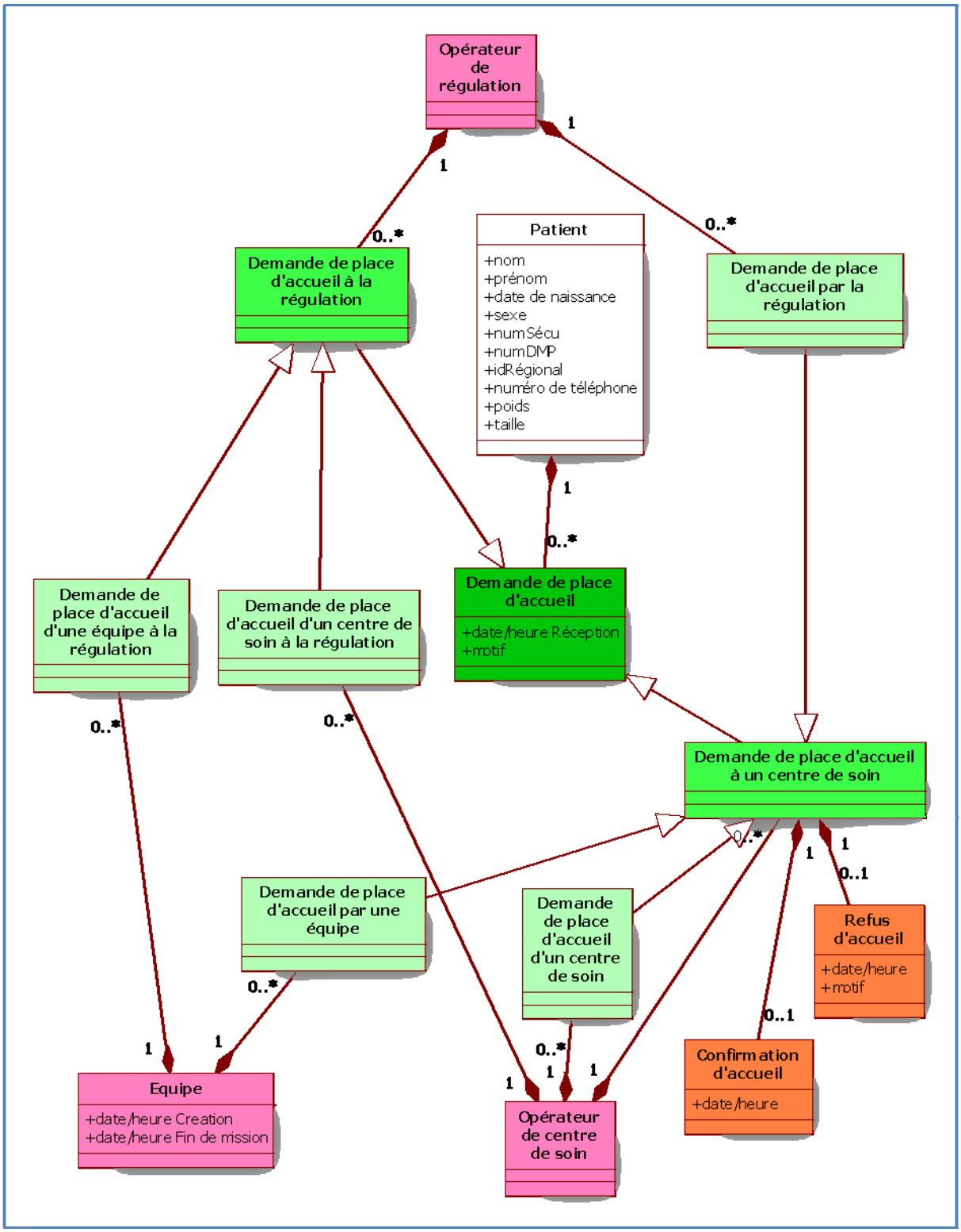


Figure 9 - Diagramme place d'accueil

PLANNIFICATION DES INTERVENTIONS PROGRAMMEES

Une intervention programmée (Figure 12) sur un patient, peut-être planifiée à l'avance par un opérateur, qui note la date et l'heure prévue de cette intervention. Une équipe peut par ailleurs être préétablie pour cette intervention, mais elle n'engage à rien sur la constitution de l'équipe finalement envoyée.

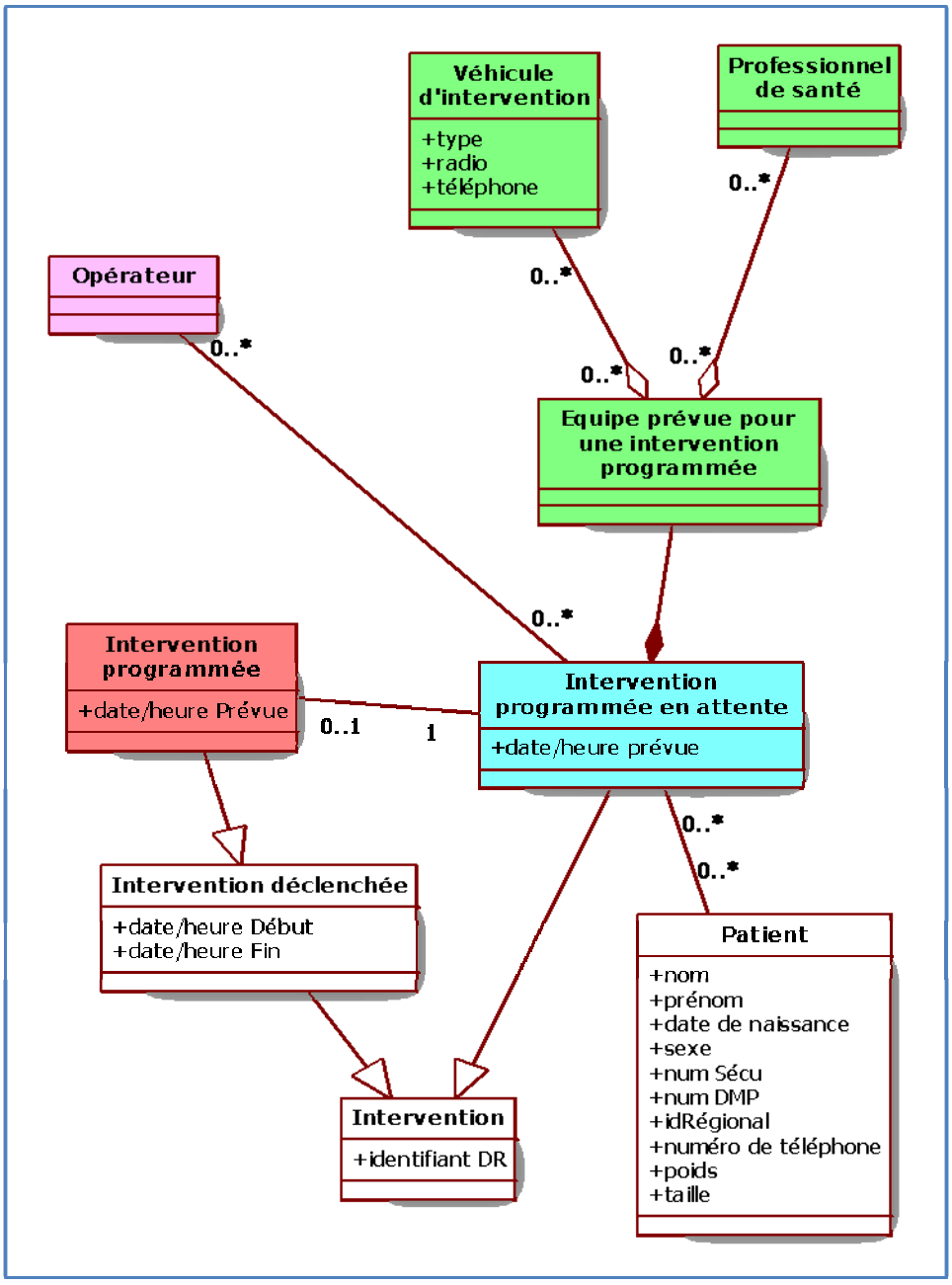


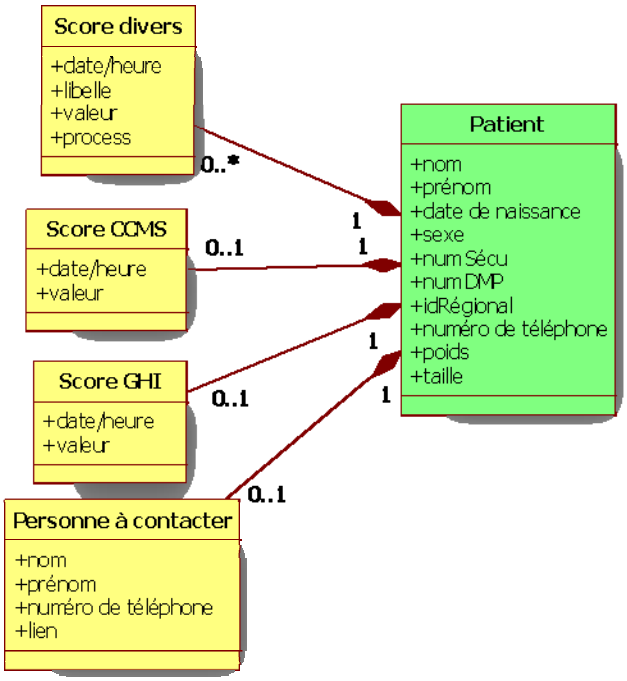
Figure 10 - Diagramme intervention programmée

LA PRISE EN CHARGE DES PATIENTS

LE PATIENT

Chaque intervention donne lieu à la prise en charge d'un ou plusieurs patients. Pour chaque patient, on renseigne les informations personnelles suivantes :

- son nom ;
- son prénom ;
- sa date de naissance ;
- son sexe ;
- son numéro de sécurité sociale ;
- son numéro de Dossier Médical Personnel ;
- son identifiant régional (si existant) ;
- son numéro de téléphone ;
- son adresse complète :
  - numéro ;
  - rue ;
  - code postal ;
  - commune ;
  - pays.



On note également les données corporelles suivantes :

- son poids ;
- sa taille.

Par ailleurs, on note aussi les informations d'un proche à contacter si nécessaire :

- son nom ;
- son prénom ;
- son numéro de téléphone ;
- son lien avec le patient.

LES SCORES DE PRISE EN CHARGE

Divers scores de prise en charge peuvent être attribués à un patient. On note en particulier :

- le score CCMS ;
- le score GHI.

Le score CCMS, qui remplace l'ancien score GEMSA, permet d'évaluer la charge de travail de la prise en charge du patient. Sa valeur varie de 1 à 6 comme précisé dans le tableau ci-joint.

Valeur	Signification
1	Malade stable ne nécessitant aucun geste thérapeutique ni diagnostique, ni de surveillance sur les lieux.
2	Malade stable nécessitant au moins un geste thérapeutique ou diagnostic ou de surveillance (traitement sur place sans transport par exemple).
3	Etat clinique pouvant s'aggraver sans mise en jeu du pronostic vital.
4	Pronostic vital ou fonctionnel immédiatement engagé sans nécessité de geste de réanimation vitale.
5	Pronostic vital engagé avec nécessité de gestes de réanimation vitale.
6	Victime décédée avant l'arrivée des secours, pas de geste de réanimation engagé.

Figure 11 - Score CCMS

Le score GHI, qui remplace l'ancien score CCMU, permet d'évaluer la charge globale de chaque patient. Celui-ci peut prendre une valeur allant de 1 à 5 :

Valeur	Signification
1	Intervention « blanche », patient décédé avant manœuvre de réanimation.
2	Intervention « non médicalisée », patient transporté non médicalisé, laissé sur place ou refusant son transport.
3	Patient transporté aux urgences ou à la maternité.
4	Patient hospitalisé en USIC.
5	Patient hospitalisé en réanimation, au bloc opératoire, sur un pôle technique spécialisé, ou décédé après manœuvre de réanimation.

Figure 12 - Score GHI

PRISE EN CHARGE SUR PLACE

La prise en charge sur place (Figure 15) est réalisée par une équipe mobile, rendue sur les lieux de l'intervention. On distingue trois types de prise en charge sur place :

- le suivi de l'état ;
- la médicalisation ;
- le transport.

LE SUIVI DE L'ETAT DES PATIENTS

Le suivi de l'état d'un patient se fait via des points de données biomédicales. A un instant donné, on peut enregistrer :

- sa température corporelle ;
- sa tension artérielle :
  - systolique :
    - à droite ;
    - à gauche.
  - diastolique :
    - à droite ;
    - à gauche.
- son taux d'oxymétrie (SaO2) ;
- sa capnographie (CO2) ;
- sa fréquence cardiaque ;
- sa fréquence respiratoire ;
- son Echelle Visuelle Analogique (estimation de la douleur).

Pour chaque point patient peuvent être associées une ou plusieurs pièces jointes, qui sont des fichiers illustrant son état (électrocardiogramme, …).

A tout moment, une observation purement textuelle peut être notée à propos du patient. Ces observations peuvent être du type :

- HDM : historique de la maladie en cours ;
- INIT : examen clinique initial ;
- EVO : évolution clinique ;
- AVIS : avis médical.

En fonction des données biomédicales du patient et des observations, un diagnostique peut être fait. Ce diagnostique est identifié par son code CIM10, à choisir dans le thésaurus SFUM. On précise également le type de diagnostique :

- Diagnostique principal (unique) ;
- Diagnostique secondaire ;
- Antécédents ;
- Motif de recours aux soins.

MEDICALISATION

Grâce à ces diagnostiques peuvent alors être prescrits des soins. Une prescription ne peut être réalisée que par un médecin, tout soin non-prescrit réalisé par un secouriste ou un infirmier étant considéré comme prescrit par cette même personne.

On distingue trois types de soins :

- les soins de secours (pouvant être réalisés par un secouriste) ;
- les soins infirmiers (pouvant être réalisés par un infirmier) ;
- les soins médicaux (pouvant être réalisés par un médecin).

Dans le cas d'un soin médical, celui-ci est identifié par son code CCAM. Le libellé de l'acte peut sinon être saisi en texte libre. On note à part la localisation du soin sur le patient. Tout soin possède par ailleurs un score TISS, qui sert à la recherche clinique.

Un soin peut être accompagné d'une prise d'un ou plusieurs médicaments. On note alors :

- le code DCI du médicament ;
- sa posologie et son unité de posologie ;
- sa voie d'administration.

Un médecin peut également réaliser une ordonnance pour un patient. A la différence de la prescription, qui concerne un soin réalisé par un professionnel de santé, l'ordonnance implique un traitement réalisé par le patient lui-même sur une certaine durée. Pour chaque ordonnance, on note :

- le code DCI du médicament ;
- sa posologie et son unité de posologie ;
- sa voie d'administration ;
- la durée du traitement ;
- la fréquence de prise du médicament.

TRANSPORT

Le transport d'un patient est enregistré de la même manière qu'un déplacement d'équipe, on note donc :

- la localisation de départ ;
- l'heure de départ ;
- la localisation d'arrivée ;
- l'heure d'arrivée ;
- le motif du transport.

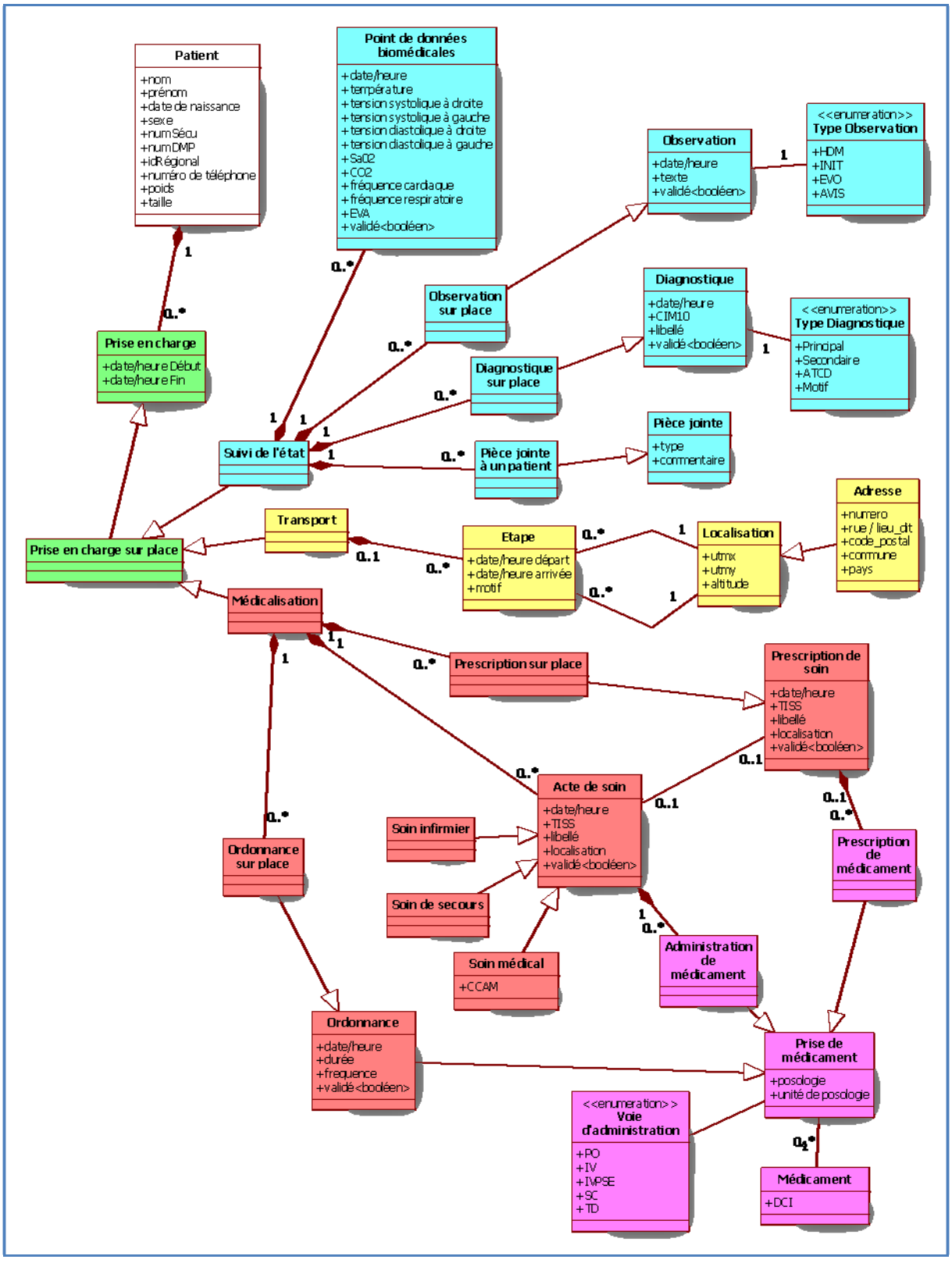


Figure 13 - Diagramme de prise en charge sur place

PRISE EN CHARGE A DISTANCE

La prise en charge à distance (Figure 16) est réalisée par une équipe distante, constituée généralement d'un unique membre, de n'importe quel type d'unité. Elle peut effectuer, de la même manière que lors d'une prise en charge sur place :

- une observation ;
- un diagnostique ;
- une prescription ;
- une ordonnance ;
- un conseil médical (pour les PARM).

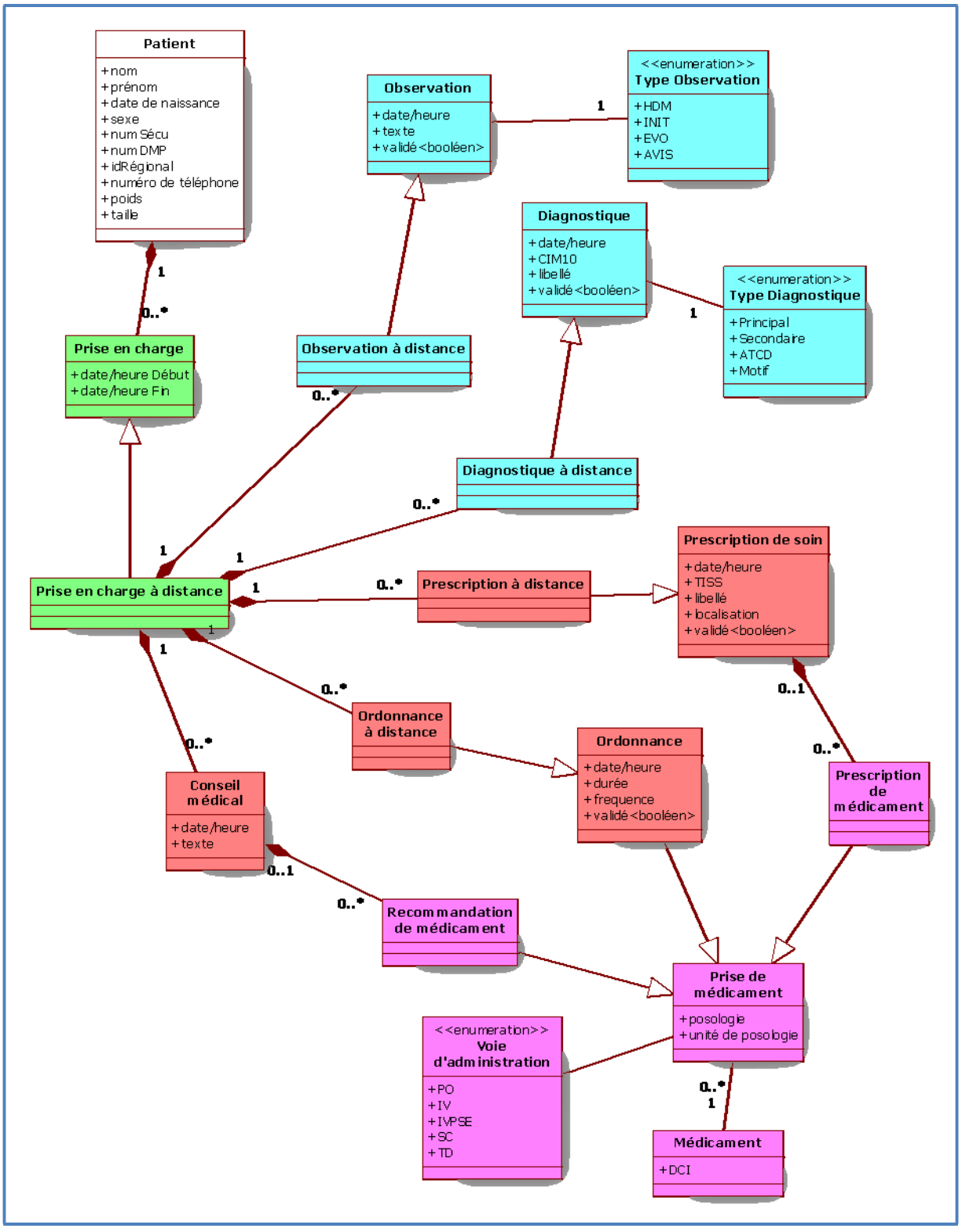


Figure 14 - Diagramme de prise en charge à distance

ENREGISTREMENT ET VALIDATION DES PRISES EN CHARGE

Toute prise en charge est signée par un membre de l'équipe (Figure 17). Cette signature implique la responsabilité du professionnel de santé l'ayant réalisée. Lorsqu'une prise en charge est enregistrée, elle n'est cependant pas obligatoirement signée de la personne qui l'enregistre. Cette dernière peut attribuer la prise en charge à un autre membre de son équipe.

Si la prise en charge est enregistrée par la personne qui la signe, elle est automatiquement validée. Sinon, celle-ci devra être validée tôt ou tard par la personne désignée lors de l'enregistrement. Une prise en charge non-validée peut être modifiée par n'importe quel membre de l'équipe. Sitôt qu'elle est validée, elle est alors verrouillée, et ne peut plus être modifiée que par la personne qui l'a signée.

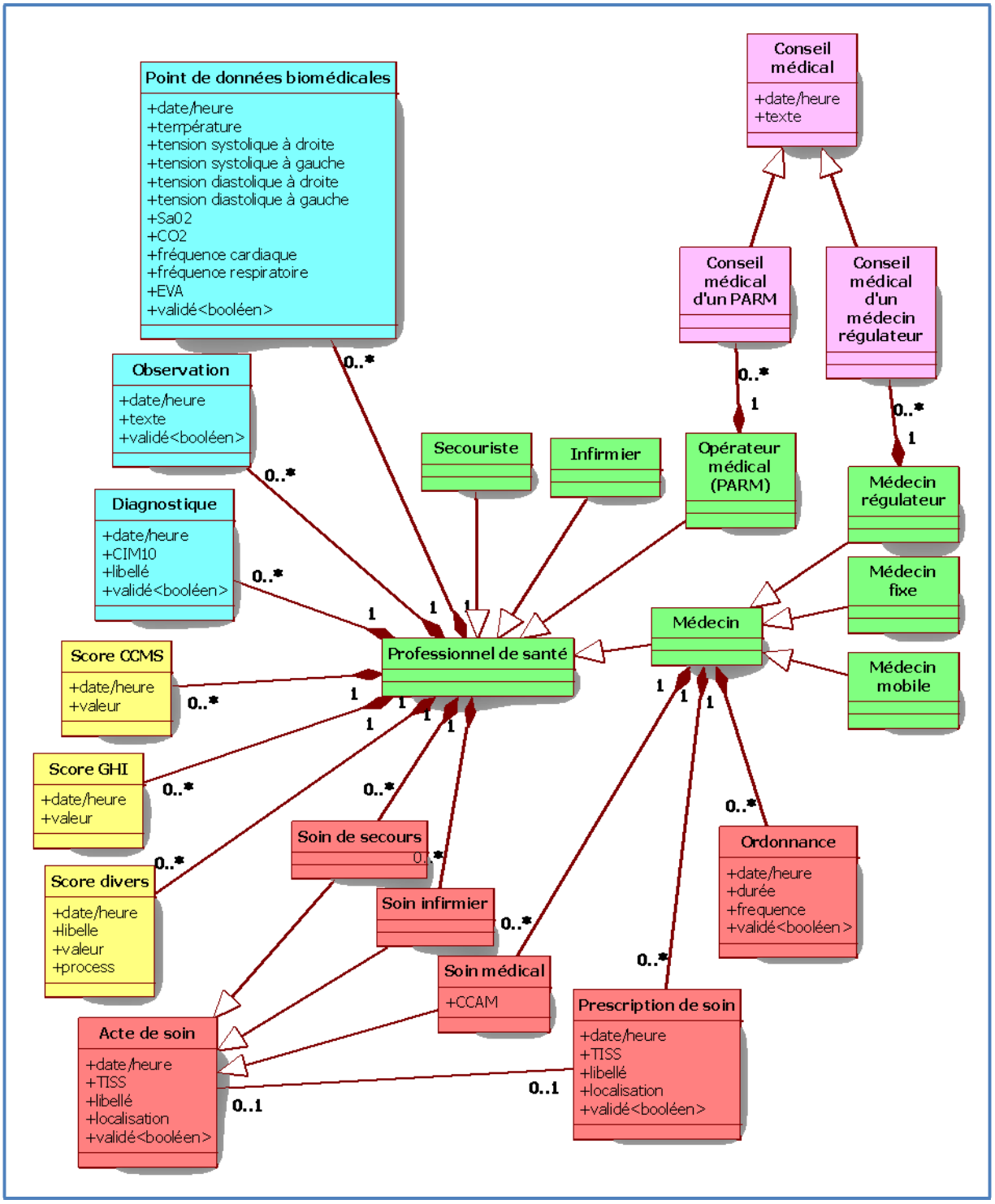


Figure 15 - Diagramme professionnel de santé

LA GESTION DES CATASTROPHES

Dans le cas d'une catastrophe, le nombre important de patients oblige une gestion plus simple et plus rapide de ceux-ci. Pour chaque patient est donc effectué un diagnostique rapide en texte libre, et la gravité de son état est estimée selon le barème suivant :

- UA : urgence absolue ;
- UR : urgence relative ;
- EU : extrême urgence ;
- DCD : patient décédé ;
- UD : urgence dépassée ;
- IMP : patient impliqué mais physiquement indemne.

Une gestion de la prise en charge des patients telle que détaillée précédemment est néanmoins toujours possible.

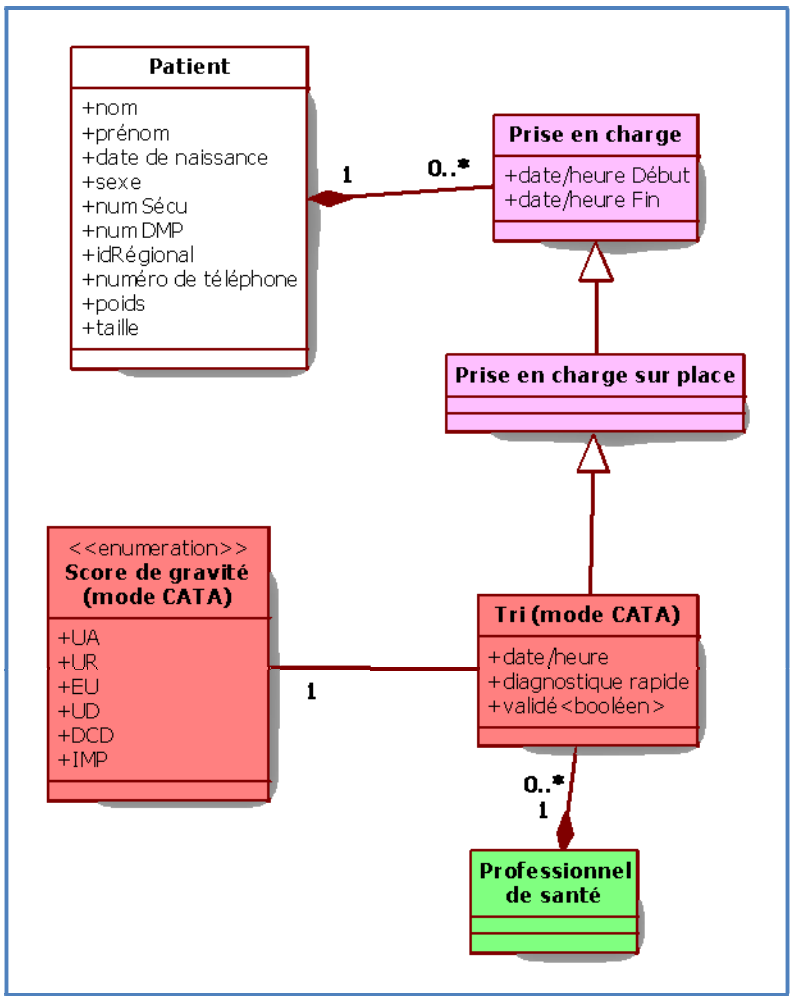


Figure 16 - Diagramme gestion catastrophe

MISE EN SITUATION – CAS D'USAGES

Pour terminer cette première présentation du cas d'étude fourni par l'IFREMMONT, nous mettons en situations les principaux objets qui vous ont été présentés dans le document. Chaque opération fera l'objet d'un diagramme de séquence dans un second document que nous prévoyons de livrer au groupe de travail à la fin du mois de juillet.

LES UTILISATEURS DU SI PREHOSPITALIER

Le cas d'usage vous rappelle le découpage en « OPERATEUR » et « PROFESSIONNEL de SANTE » présenté en début de document et introduit une notion supplémentaire « ADMINISTRATEUR ». Un administrateur a deux niveaux possibles : administrateur d'unité (au sens de l'unité définit plus haut dans le document) et/ou administrateur global du SI pré hospitalier.

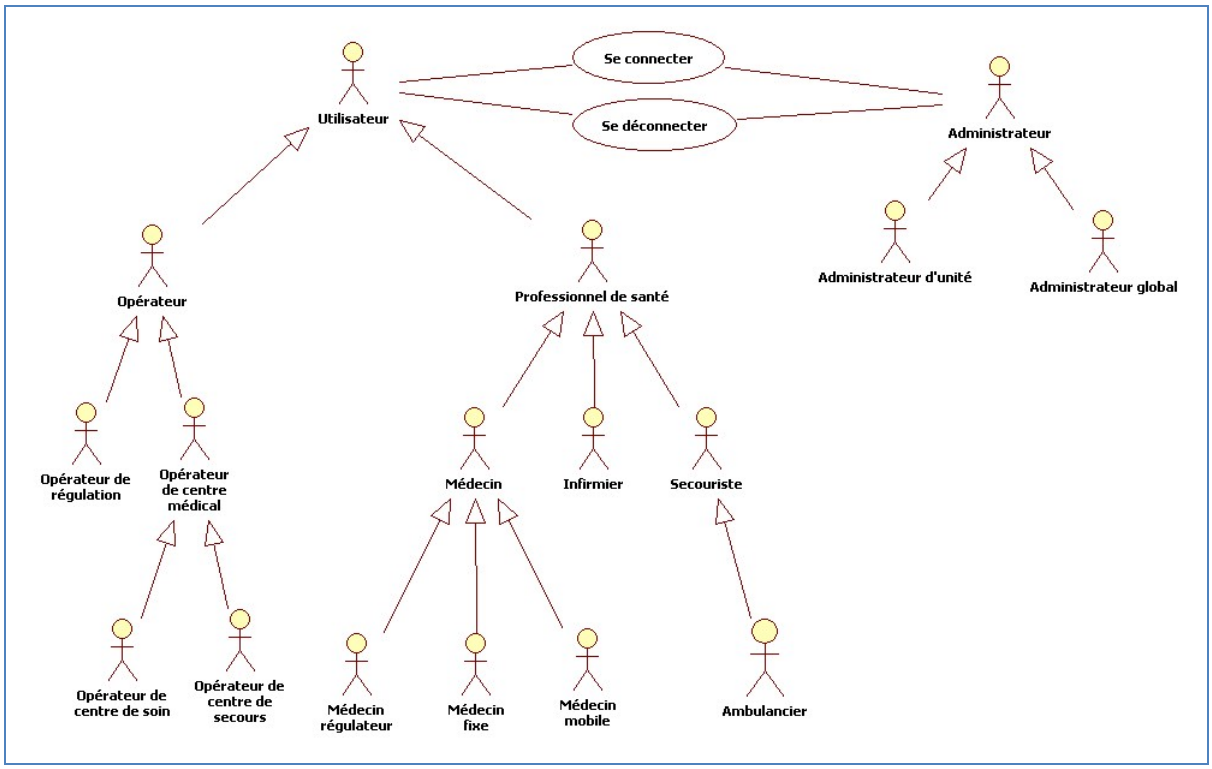
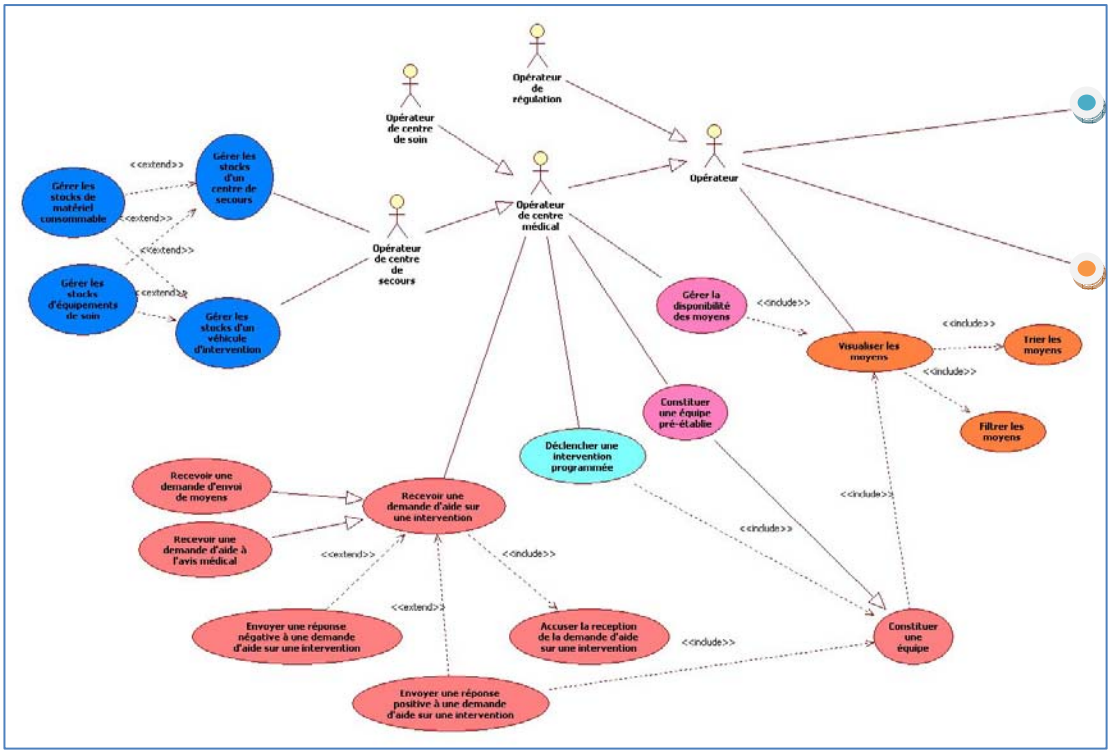


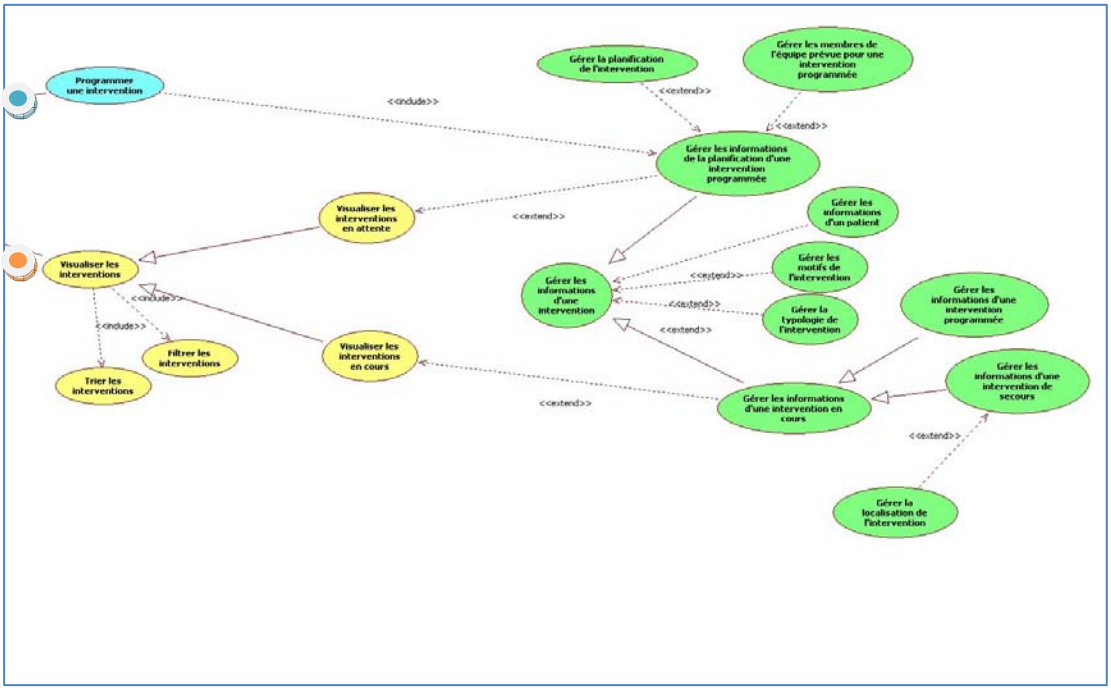
Figure 17 - Cas d'usage utilisateurs

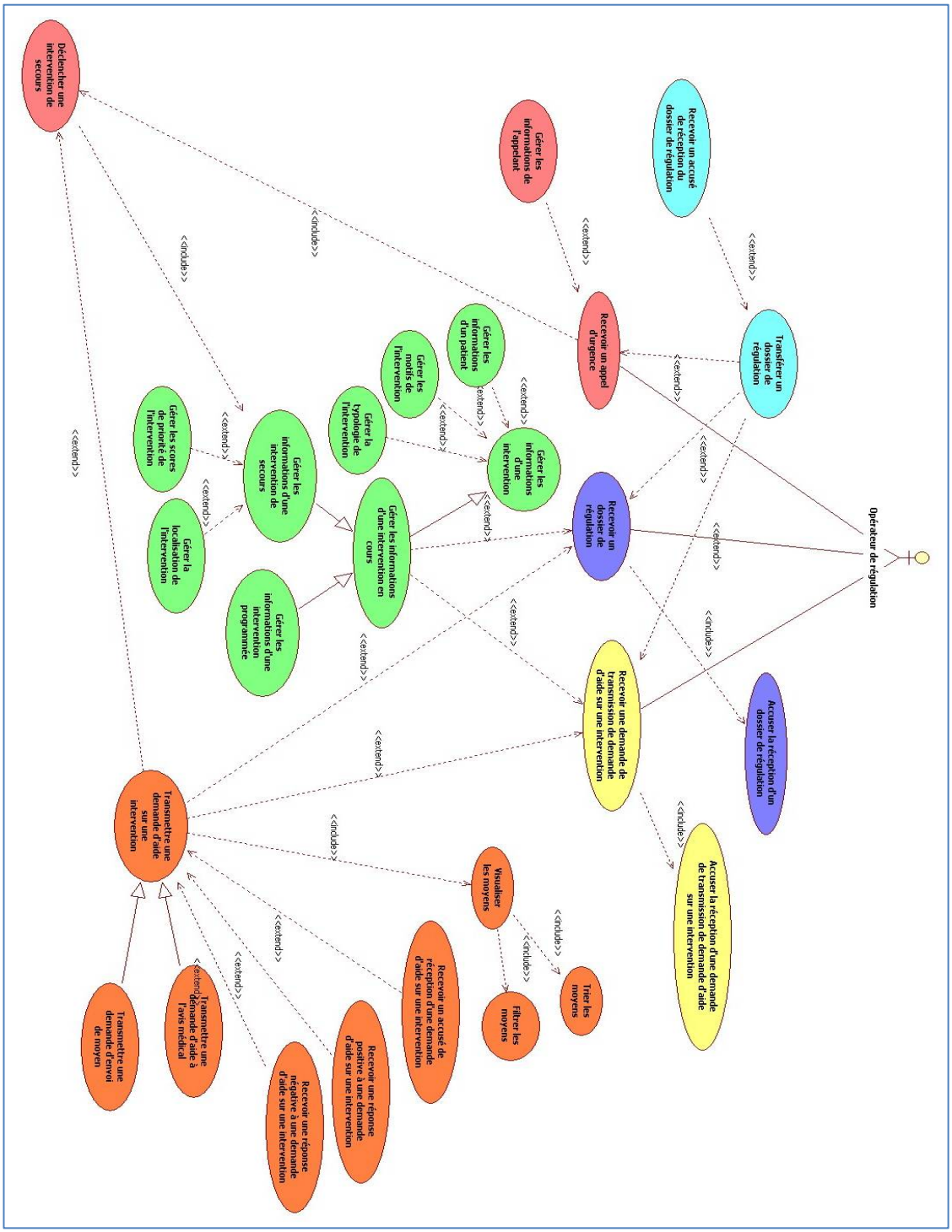
Deux opérations sont donc à prendre en compte, « SE CONNECTER » et « SE DECONNECTER » qui vont mettre en jeu (cf. Figure 2 et Figure 3) les objets « MOYEN HUMAIN », « PERSONNE » et « UTILISATEUR SI » et leurs dérivés. C'est à ce niveau que vont être attribués les droits et associations d'objets du SI.

Le but est d'avoir un état des lieux centralisé sur le SI pré hospitaliers, des utilisateurs et de leur répartition.

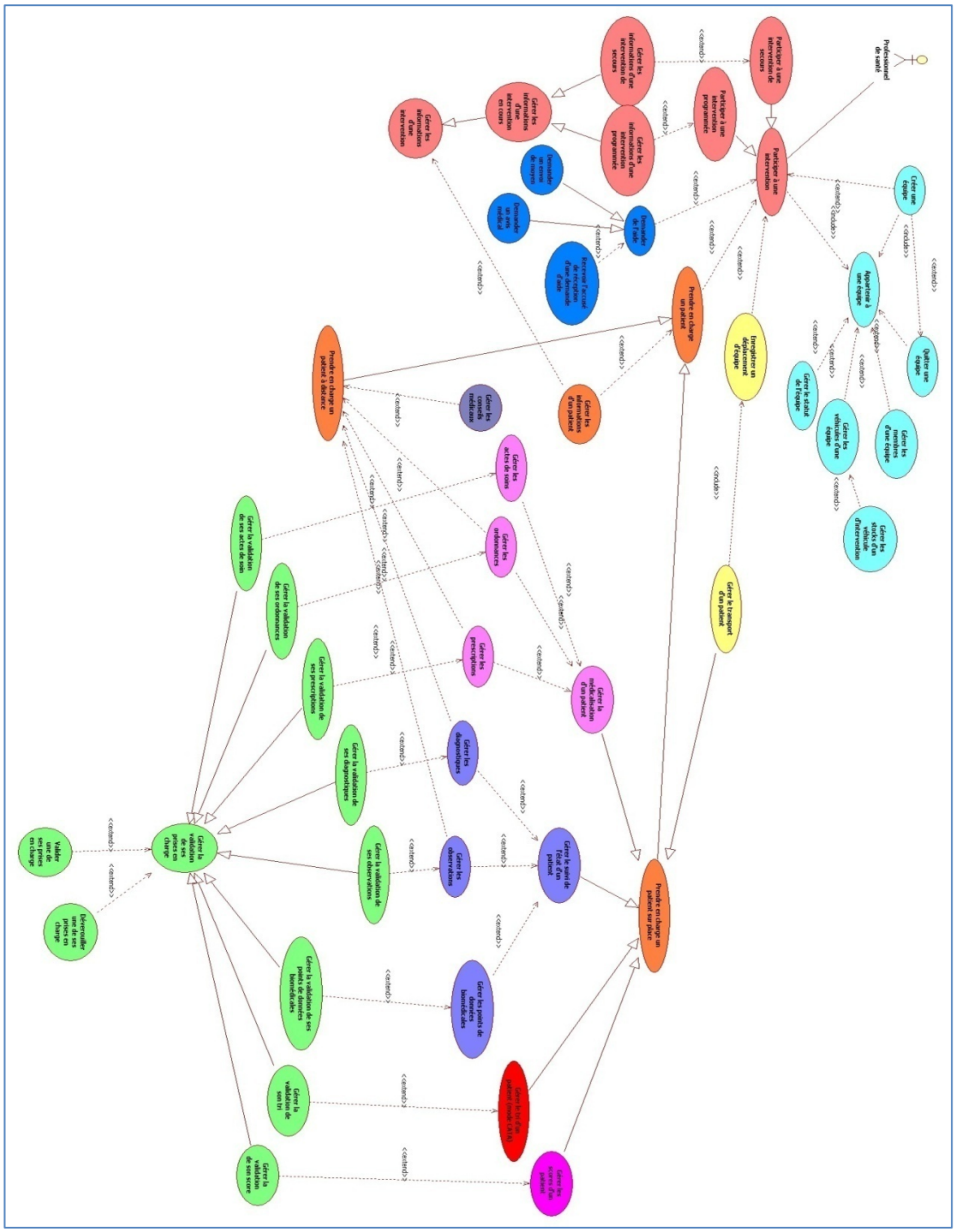
FONCTIONS D'UN OPERATEUR






Déclencher une intervention de secours
Recevoir un accusé de réception du dossier de régulation
Gérer les informations de l'appelant
Recevoir un appel d'urgence
Transférer un dossier de régulation
Gérer les informations d'un patient
Gérer les motifs de l'intervention
Gérer la typologie de l'intervention
Gérer les informations d'une intervention
Gérer les scores de priorité de l'intervention
Gérer les informations d'une intervention de secours
Gérer la localisation de l'intervention
Gérer les informations d'une intervention en cours
Gérer les informations d'une intervention programmée
Recevoir un dossier de régulation
Opérateur de régulation
Recevoir une demande de transmission de demande d'aide sur une intervention
Accuser la réception d'un dossier de régulation
Accuser la réception d'une demande de transmission de demande d'aide sur une intervention
Transmettre une demande d'aide sur une intervention
Visualiser les moyens
Trier les moyens
Filtrer les moyens
Recevoir un accusé de réception d'une demande d'aide sur une intervention
Recevoir une réponse positive à une demande d'aide sur une intervention
Recevoir une réponse négative à une demande d'aide sur une intervention
Transmettre une demande d'envoi de moyen
Transmettre une demande d'aide à l'avis medical
<<include>>
<<extend>>

FONCTION PROFESSIONNEL DE SANTE



CONCLUSIONS

Cette première description permet de bien visualiser la complexité des flux, objets, données échangées dans un SI pré hospitalier. Cette rédaction a été programmée dans le cadre du refactoring du projet initial du Res@mu. Ce découpage doit permettre d'appliquer la méthodologie SELKIS à ce cas d'étude.

SI tout se passe bien nous obtiendrons une modélisation plus efficiente et dont la sécurisation sera accrue. Nous pourrons ensuite en tirer un nouveau SDK aboutissant à la création de nouveaux profils IHE afin d'offrir une réelle interopérabilité aux différents acteurs du pré hospitaliers.

Chapitre 3

Besoins de sécurité pour l'application Res@mu

Cette section donne quelques éléments identifiés lors de la réunion du 8 septembre 2009 à Chambéry et qui réunissait
– Akram Idani
– Mohamed-Amine Labiadh
– Yves Ledru
– Jean-Luc Richier
– Quentin Switsers
– Pascal Zellner
La réunion a consisté en une présentation de la méthode KAOS, une revue détaillée du modèle des données UML préparé par IFREMMONT, et une discussion sur les besoins de sécurité. Les prochains paragraphes se concentrent sur l'identification de ces besoins de sécurité.

Ils comprennent :

1. L'identification de la cible de sécurité
2. L'identification des différents types d'utilisateurs du système (rôles)
3. L'identification des propriétés de sécurité de haut niveau (ACIT) applicables à la cible de sécurité

3.1 Cible de sécurité

Le système Res@mu enregistre de nombreuses données qui doivent être protégées. Cependant, dans le cadre de cette expérimentation pilote, la cible de sécurité se limitera aux données les plus sensibles, qui sont constituées par les données médicales du patient. Ces données sont stockées dans la classe ManagementAct et dans ses sous-classes. Un objectif majeur est celui de l'intégrité des données : il faut s'assurer que les données manipulées restent les mêmes.

Par ailleurs, Res@mu prévoit une forte traçabilité des activités menées au travers du logiciel. Cela a notamment un intérêt vis-à-vis de la facturation correcte des actes réalisés.

En résumé, le choix de ManagementAct comme cible de sécurité revient à sélectionner ce qui a le plus de valeur :
– Sur le plan médico-légal
– Sur l'exigence d'intégrité
– Sur le plan économique (justification des factures).

3.2 Les rôles

Le diagramme ci-dessous (Fig. 3.1) identifie et structure les différents types d'utilisateurs du système. Il s'agit en fait de rôles car une même personne peut être amenée à jouer plusieurs rôles différents dans des sessions différentes. Par exemple, un médecin peut certains jours jouer le rôle de médecin régulateur, et d'autres jours, jouer le rôle de médecin dans une équipe de secours.

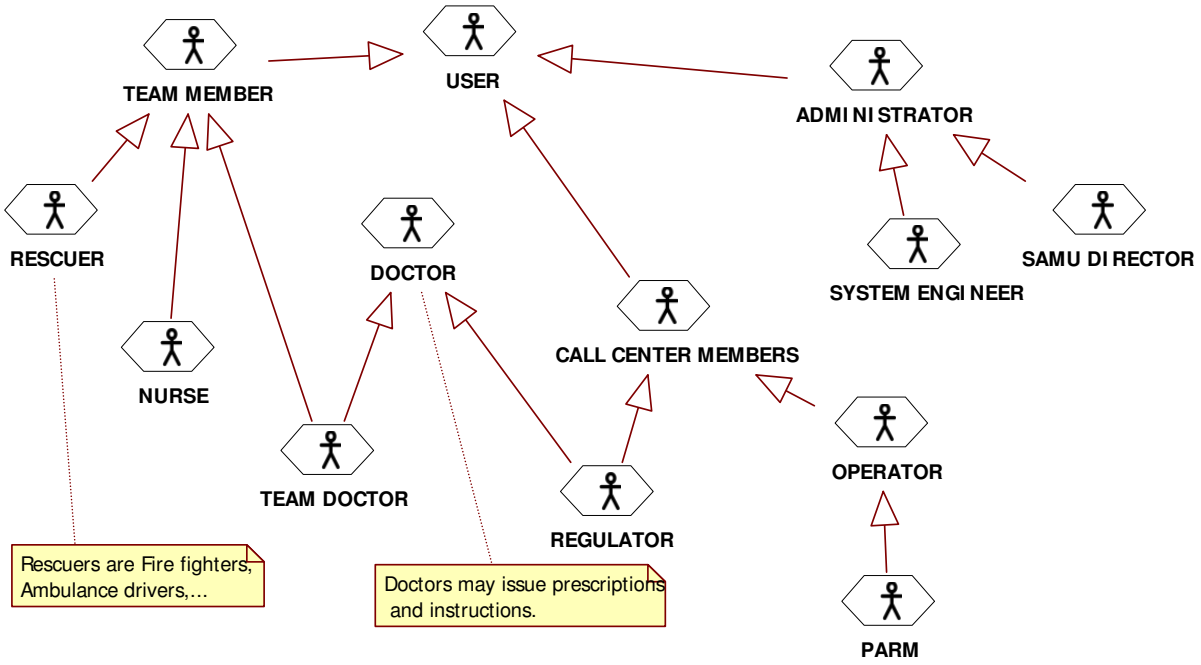


FIGURE 3.1 – Les rôles dans l'application Res@mu

Ces rôles sont organisés dans une hiérarchie de spécialisation. La plupart des rôles qui sont spécialisés sont des rôles "abstraits", c'est-à-dire qu'aucun utilisateur du système ne se connectera sous ce rôle, mais en utilisant un sous-rôle. Seul le rôle OPERATOR fait exception à cette règle : on peut se connecter comme OPERATOR ou comme PARM.

Voici une description de chacun de ces rôles :

USER : le rôle USER est un rôle générique qui regroupe tous ceux qui ont accès au système Res@mu via une de ses interfaces.

ADMINISTRATOR : Les administrateurs ne participent pas aux interventions d'urgence, mais ils effectuent des opérations techniques liées à la bonne administration du système. Ils jouissent de privilèges qui leur donnent accès à la plupart des données et des opérations du système, mais ils doivent les utiliser à bon escient. Leurs actions sont tracées, ce qui permettrait de détecter d'éventuels abus.

SYSTEM ENGINEER : Il est en charge des tâches techniques liées à l'administration de l'application.

SAMU DIRECTOR : En tant que directeur du SAMU, il est responsable des actions menées par ses équipes. Il n'effectue des tâches d'administration que dans un but de contrôle ou pour

satisfaire des obligations légales (demande de la justice) ou médicales (demande d'un directeur d'hopital). C'est le cas, par exemple, quand une autorité judiciaire requiert une information contenue dans RES@MU.

CALL CENTER MEMBER : Ce sont les personnes qui répondent au téléphone lors d'un appel au SAMU. Selon leur qualification, elles peuvent réaliser certains actes médicaux (ManagementAct).

OPERATOR : c'est la personne qui répond en premier à l'appel. Cette personne n'a pas de formation médicale spécifique, mais est liée par le secret médical. Elle est chargée de collecter les éléments factuels sur le patient (état civil, lieu de l'accident,...) avant de passer l'appel à une personne qui a une formation médicale. L'opérateur n'a a priori pas accès aux données médicales du patient.

PARM : c'est un opérateur qui a reçu une formation médicale spécifique (Permanencier Auxiliaire de Régulation Médicale). Cette formation lui permet de donner des conseils médicaux, qui constituent une forme de ManagementAct. Si l'appel requiert des actes médicaux plus importants, il sera transféré à un médecin.

DOCTOR : Les médecins ont le droit de réaliser ou de prescrire des actes médicaux. Ils en assument également la responsabilité. Ils peuvent se trouver au centre d'appel (médecin régulateur) ou dans l'équipe de secours (team doctor).

REGULATOR : Après qu'un opérateur ou un PARM ait pris les informations factuelles sur le patient, et en fonction de l'urgence, son appel est transféré au médecin régulateur. Celui-ci a la responsabilité d'apporter une réponse en adéquation avec le problème du patient. Cette réponse peut consister en une prise en charge à distance (consultation par téléphone, suivie d'un conseil médical, d'une ordonnance ou d'une prescription) ou en une prise en charge sur place par une équipe dépéchée sur les lieux. Dans ce cas, le médecin régulateur est responsable du choix de l'équipe, de la modification éventuelle de cette équipe pendant l'intervention, du suivi des interventions en cours, de la sélection éventuelle d'un lit d'hopital où envoyer le patient. Il a également la possibilité de réaliser des actes à distance pendant l'intervention (par exemple, une prescription ou une ordonnance). Il faut noter qu'en France, un médecin régulateur ne peut pas être mobile, alors que dans d'autres pays (par exemple en Italie), il a le droit d'aller sur le terrain.

TEAM MEMBER : ce sont les membres des équipes de secours envoyées auprès du patient. Tous les membres des équipes de secours participant à une intervention ont accès aux informations médicales du patient, y compris après avoir confié le patient à une autre équipe ou une autre organisation. Par contre, les membres de l'équipe de secours ne peuvent modifier les données médicales du patient que pendant l'intervention. Une équipe de secours n'est responsable que d'un seul patient à la fois.

RESCUER : le secouriste est un membre de l'équipe d'intervention qui n'a qu'une formation médicale réduite. Il s'agit typiquement des ambulanciers ou des pompiers. Il ne peut pas réaliser d'acte médical. Selon les départements, on peut envisager de restreindre leur accès aux données médicales du patient pris en charge et le limiter au seul état civil du patient.

NURSE : Les infirmiers ont reçu une formation médicale qui leur permet de réaliser des actes sur ordre d'un médecin (qui en prend la responsabilité).

TEAM DOCTOR : Le médecin de l'équipe de secours réalise ou demande les actes médicaux. Il a la responsabilité des actes réalisés par son équipe.

Les TEAM MEMBERs et CALL CENTER MEMBERs sont tous des **acteurs préhospitaliers**.

A noter également que cette hiérarchie se concentre sur les **rôles** joués par les différents utilisateurs de RES@MU. Cette notion est différente de la notion d'agent proposée par KAOS (qui comprend des agents logiciels ou matériels, voire des agents qui n'intéragissent pas directement avec le système). Par contre, cette notion de rôle est proche de la notion d'acteur apparaissant dans les use cases. Les acteurs des use cases intéragissent directement avec le système. Notons cependant que certains acteurs des use cases peuvent être logiciels ou matériels.

A noter que les patients et leurs familles n'ont pas d'accès direct au système RES@MU. Ils ne sont pas utilisateurs du système et doivent passer par des intermédiaires pour fournir de l'information à RES@MU ou sortir de l'information du système. Quand il s'agit de sortir de l'information du système, ce sera généralement via les administrateurs, et en particulier via une demande officielle au directeur du SAMU.

3.3 Propriétés ACIT relatives à ManagementAct

Le but de cette section est d'identifier les besoins de sécurité pour la cible ManagementAct en ce qui concerne les quatre propriétés de haut niveau ACIT (Availability, Confidentiality, Integrity, Traceability).

Confidentialité : Les données médicales enregistrées dans ManagementAct sont protégées par le secret médical. Elles sont protégées contre toutes les personnes qui ne participent pas ou n'ont pas participé à l'intervention. Seuls les membres des équipes de terrain qui ont participé à l'intervention sur un patient, ainsi que les PARM et régulateur(s) du call center qui ont participé à l'intervention ont accès à ces données médicales. Les administrateurs y ont également accès mais dans la mesure où leurs obligations de service leur demandent d'avoir un tel accès. Des restrictions peuvent s'appliquer aux secouristes (rescuers) et opérateurs selon le département où ils exercent.

Par contre, l'accès à ces informations confidentielles reste garanti après que l'intervention soit terminée dans un but de formation des équipes sur base de ce retour.

On notera qu'une façon de casser la confidentialité est de modifier la composition d'une équipe a posteriori. Seul le médecin régulateur a le droit de demander l'ajout d'une équipe à une intervention (en faisant une demande d'aide à une unité qui enverra l'équipe) pendant l'intervention. Il n'est plus possible de modifier une équipe une fois l'intervention terminée. Par contre, il est possible de transférer des personnels d'une équipe à une autre pendant l'intervention, pour deux équipes associées à l'intervention (même si elles travaillent sur des patients différents).

Availability : Les équipes et membres du call center qui participent ou ont participé à une intervention peuvent et doivent avoir accès aux données médicales. Ils ont le droit d'ajouter de l'information pendant l'intervention, et seulement de la consulter après la fin de l'intervention. Les administrateurs ont seulement un droit de consultation.

Intégrité : L'intégrité des données médicales est un besoin très fort de l'application Res@mu. Il faut éviter de détruire ou de modifier des données médicales, ou de les corrompre pendant

leur transfert ou recopiage. La plupart des opérations proposées ne permettent pas de modifier des données de type ManagementAct, mais simplement de les créer et de les ajouter au dossier du patient.

Plusieurs cas d'utilisation correspondent à des besoins forts d'intégrité :
- la validation d'un ManagementAct doit être réalisée par la personne responsable de ce ManagementAct. Il faut éviter qu'un acte soit validé par une personne autre que son responsable. Ceci constituerait une brêche à l'intégrité des données. Dans une moindre mesure, il faut éviter qu'une personne extérieure à l'intervention puisse ajouter et/ou valider un acte médical (qui n'aurait pas eu lieu).
- Même si il n'est possible que de créer de nouveaux actes, il faut s'assurer qu'on ne perd pas les liens déjà établis entre un patient et les actes qui le concernent. Ceci concerne notamment la commande qui permet d'ajouter ou de créer un management act pour un patient donné.
- Des erreurs de saisie sont toujours possibles. Il est important de pouvoir les corriger. Cela concerne d'une part des actes qui auraient été validés mais dont la description est erronnée, et d'autre part des actes qui seraient rattachés à un autre patient que celui qui a reçu cet acte.

Traçabilité : Il a déjà été mentionné que la traçabilité est une propriété essentielle de ce nouveau système. En ce qui concerne ManagementAct, la traçabilité permet d'éviter des abus, en particulier en matière de consultation abusive de données confidentielles. Elle permet également de facturer les actes réalisés par le SAMU. A priori, on peut imaginer que toutes les actions réalisées feront l'objet d'un enregistrement et que la traçabilité sera fournie comme un mécanisme sous-jacent à Res@mu.

3.4 Menaces

Pour l'instant, les SAMU n'ont pas fait l'objet d'attaques informatiques. Le seul acte répertorié est l'introduction d'un virus par la clé USB d'un des membres du call center.

A priori, il n'y a pas d'acteurs extérieurs malveillants, même si on peut imaginer que certains acteurs externes (compagnie d'assurance, famille d'un patient) pourraient vouloir avoir accès à un dossier en dehors des voies légales. Pour la famille, la voie légale d'accès au dossier, c'est la justice.

En ce qui concerne les acteurs habilités à avoir accès au système :
- L'administrateur système peut faire beaucoup de choses et avoir accès à de nombreuses informations si elles ne sont pas cryptées.
- Le directeur du SAMU a un droit exceptionnel de consulter et il donne le résultat de sa consultation à un officier de police judiciaire, si il s'agit d'une demande de la justice, ou au directeur de l'hopital, si il s'agit d'une demande médicale.
- Dans le cas d'une intervention, on demande au patient si il est d'accord de transmettre une copie du dossier au médecin de famille.
- Si les acteurs habilités à avoir accès au système font une consultation abusive, elle sera tracée.
- Si les acteurs habilités à avoir accès au système font une modification abusive, elle sera tracée. De toutes façons, ils ont peu d'intérêt à faire une telle modification :
  - ajouter des actes non réalisés ne leur rapporte rien
  - ils peuvent vouloir essayer de cacher une erreur, mais leurs modifications seront tracées
  - a priori, une fois l'intervention terminée, ils ne peuvent plus rien modifier (si ce n'est valider).

3.5 Conclusion

Dans cette section, nous avons identifié les principaux rôles que peuvent prendre les utilisateurs de Res@mu. Nous avons également identifié à un haut niveau de granularité les besoins de sécurité ACIT relatifs à ManagementAct.

L'étape suivante consiste à représenter ces besoins dans une hiérarchie de buts (exprimée en KAOS) et à traduire ensuite ces buts en une politique de contrôle d'accès.

Chapitre 4

Méthode utilisée pour définir une politique de contrôle d'accès

Cette section présente les principes de la méthode utilisée pour structurer les besoins de sécurité et les relier aux besoins fonctionnels dans une hiérarchie de buts KAOS. Ces besoins sont ensuite traduits en une politique de contrôle d'accès dont les règles peuvent être reliées à certains buts.

Le reste de cette section est écrit en anglais et est destiné à une prochaine publication.

4.1 Overview of the experiment

This work takes place within one of the case studies of the Selkis project dedicated to the development of secure information systems. The case study is an information system for medical urgency. It covers every stage of a medical urgency situation, from the initial call to a medical urgency center, to the management of emergency teams and vehicles during a mission. The information system will store medical data about the patients concerned by an emergency situation. The goal of the case study is to elicit security requirements about these medical data, and to describe the security policy as an RBAC model.

Our starting point is a set of UML diagrams (class diagrams and use case diagrams), prepared by IFREMMONT, which describe the information model and the major functionalities. The diagrams feature 77 classes and more than 100 use cases. The identification of security requirements for the whole information system would be a huge task, so we decided to focus on a critical issue : the protection of medical data.

In the class diagram, medical data are exclusively stored in class "ManagementAct" and its numerous subclasses (Fig. 4.1). Each Management act corresponds to a single medical act (analysis, prescription, instruction, care,...) [1]. It is linked by a composition relation to class Patient, representing the patient who received the medical act, and to class PreHospitalActor, representing the member of the medical emergency team who achieved this medical act.

Since management acts store confidential and critical information about patients. We focus on the security requirements linked to this class.

The proposed methodology builds on the KAOS method to identify and locate high level security requirements. Then, it enriches the UML class diagram with Role-Based Access Control information.

1. For simplicity reasons, we only display five subclasses of class ManagementAct. The original UML diagram features 9 subclasses.

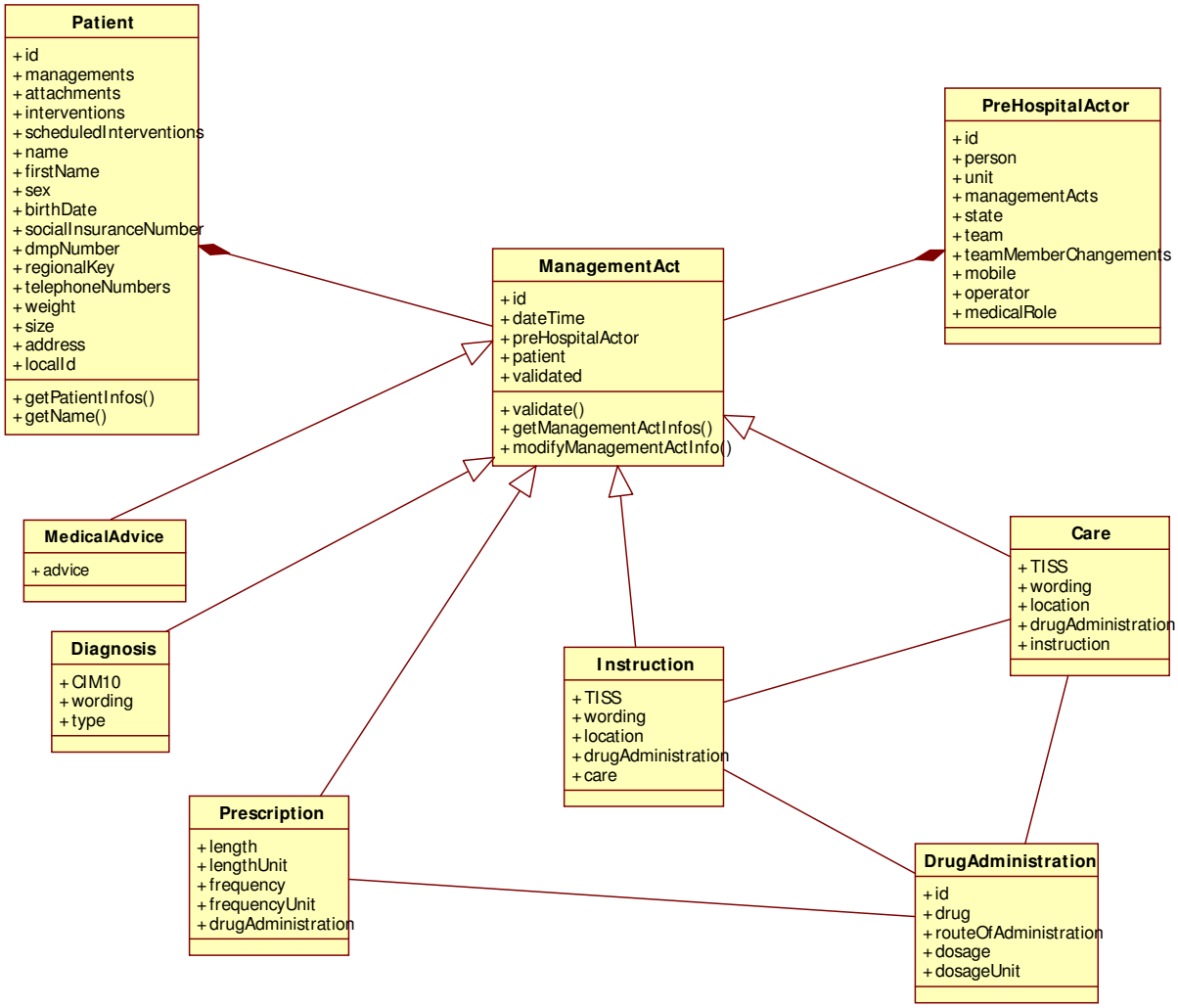


FIGURE 4.1 – Class diagram for Management Act and the relevant linked classes.

4.2 KAOS

4.2.1 Goal refinement

KAOS [2] is a goal-based requirements engineering method. The main KAOS diagram identifies a hierarchy of goals which motivate the development of the system. High level goals capture overall motivation for the system, such as business needs. Lower level goals provide more operational objectives. A refinement hierarchy leads from high level to lower level goals. These lower level goals can be distributed amongst the various agents of the system. Agents can be human beings, or software to develop.

For example, Fig. 4.2 details how a patient can be managed remotely, by phone. This corresponds to two cases :

– Medical advice : the patient makes an emergency call, but his problem is rather simple and does not require the help of a doctor. The operator on the phone simply gives some advices to the patient.

– Prescription or instruction : the patient makes an emergency call, or the call is performed by some emergency team which does not include a doctor. The phone operator must be a doctor, and he has the right to issue a prescription or an instruction for the patient to take some drug

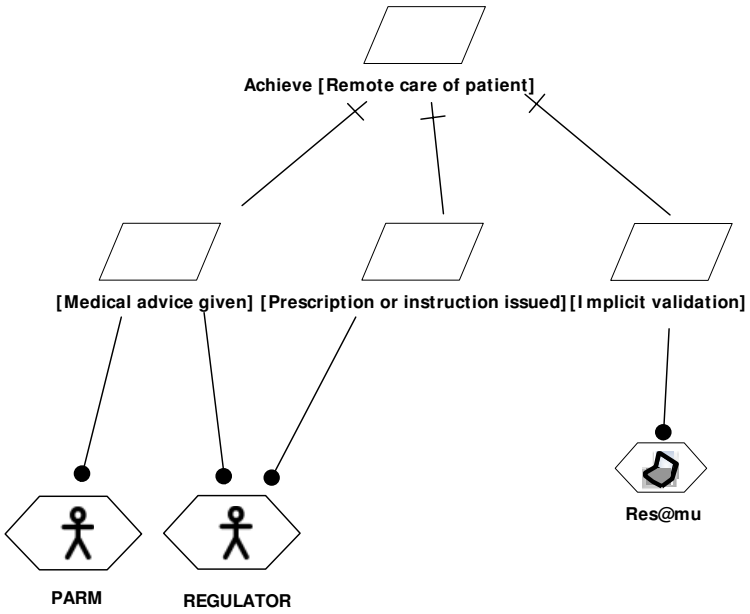


FIGURE 4.2 – Refinement of goal "remote care of patient"

or get some care from the emergency team. [2]
Medical advices, prescriptions and instructions are all management acts, and must be validated by the medical actor who took responsibility for it. In the case of remote care, these acts are entered in the system by the telephone operator, who is the person responsible for the act. Therefore, this act does not require explicit validation by the agent and is implicitly validated by the system agent, named Res@mu.

4.2.2 KAOS agents

As already mentioned, KAOS goals may be associated to agents who are responsible for fulfilling the goals. Fig. 4.3, already shown in the previous section, gives the hierarchy of roles involved in the medical urgency system. These goals give a subset of the agents which will appear in the KAOS diagrams. KAOS agents will also include non-human agents, i.e. software agents. Actually, the original KAOS method does not feature specialisation links between agents. The only link is an aggregation link. In this project, we felt the need for specialisation. For example, Fig. 4.5 features the OPERATOR agent who can either be an ordinary operator or a PARM. Our agent hierarchy also uses multiple inheritance. For example, a regulator is a call member center, i.e. a phone operator, who is also a doctor.

In Fig. 4.2, the three lower level goals are associated to agents. The goal "Medical Advice given", is associated to two agents who may give such advices : PARM and REGULATOR. Both are specialisations of call center members who are qualified for such medical advices : the regulator is a doctor, while the PARM is an operator who followed a specific training. We might have defined an abstract agent MEDICAL OPERATOR which includes both categories but this would only be used in this particular context and was not perceived as definitely needed. Here again, we deviate a little from the KAOS method which prescribes that a lower level goal must be associated to exactly one agent. Other lower level goals are associated to a human or software agent : prescriptions and instructions are issued by the regulator, and implicit validation is

2. As shown in Fig. 4.1, an instruction is always associated to a care, performed by some medical actor, which guarantees that drug administration really takes place. A prescription relies on the cooperation of the patient to take the drug as prescribed.

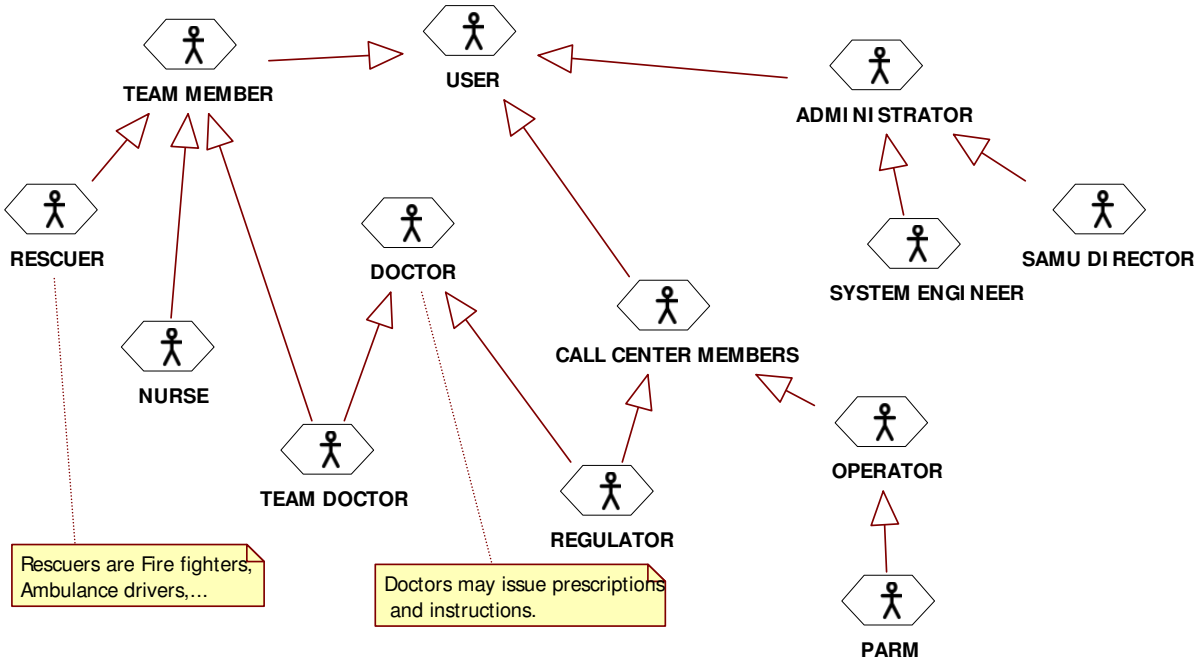


FIGURE 4.3 – Human agents of the medical urgency system

automatically performed by the system.

4.2.3 Link to the data model

KAOS goals can also be linked to the data concerned by the goal. In Fig. 4.4, we link the three lower level goals to the ManagementAct class, since they all involve the creation or modification of such objects. KAOS also allows to link goals to operations, but this feature was not be used in this case study. In a later stage, we will also express links from goals to access control rules.

4.2.4 Security goals

KAOS goals are not necessarily functional. This allows to use KAOS to express security goals. In our example, a goal can express that "medical data should be kept confidential". In the Selkis project, high level security properties are sorted into the four ACIT categories :

– Availability : security measures should not prevent the user from accessing data when needed ;
– Confidentiality : data should not be disclosed to unauthorized persons ;
– Integrity : unauthorized users should not be allowed to modify or delete data ;
– Traceability : accesses to the data by users should be logged.

Fig. 4.5 shows that the high level goal "SAMU de Qualité" includes two sub-hierarchies : a functional one and another one dedicated to security.

Availability, Confidentiality, Integrity, and Traceability (ACIT) are high level properties that must be enforced by an adequate security policy. In Selkis, we use RBAC (or variants of it) to express the rules of such policy properties.

In Role-Based Access Control (RBAC) [1], security policies are expressed by rules which express the permissions of users on resources which can be objects or operations. RBAC introduces the intermediate notion of roles between users and permissions. As a result, all users playing the same role have the same permissions, and it is possible for users to play several roles, and depending on their current role to be granted various permissions.

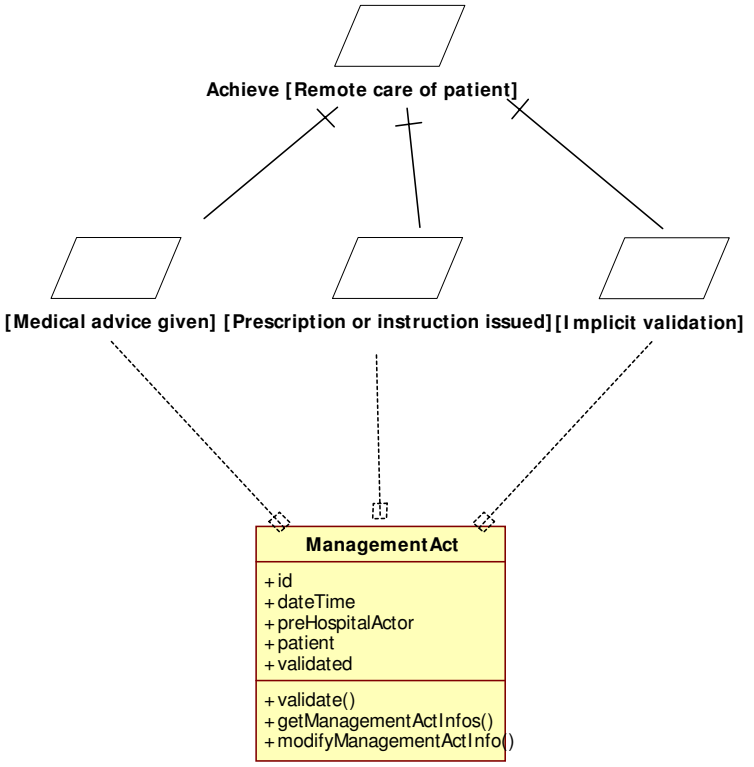


FIGURE 4.4 – Goals can be linked to classes

4.2.5 From KAOS to RBAC

Besides security goals, KAOS provides the notions of agent and links to the data. Agents are close to the RBAC notion of role, except that we except roles to correspond to human agents. Data correspond to the resources controlled by the RBAC permissions. KAOS models can thus be used as a starting point to identify the elements which define RBAC rules.

4.3 Methodology followed in our case study

We will now review the process applied to identify security requirements and define our RBAC security policy for this case study. As already mentioned, the starting point of our case study was made up of a set of class diagrams, associated to use cases. Our process was composed of the following steps :

1. Construction of an agent hierarchy from interviews with IFREMMONT.
2. Identification of use cases related to the security target, i.e. Management Acts
3. Construction of a KAOS functional goal hierarchy based on the structure of these use cases.
4. Identification of security goals linked to the data to protect (here, Management Act)
5. Identification of functional goals which are linked to the data protected by security goals. These functional goals are refined into functional sub-goals which enforce the security rules.
6. Expression of RBAC rules which enforce security goals ; these RBAC rules are linked to the corresponding KAOS goals.
7. Check that every functional goal remains satisfiable in the context of RBAC rules.

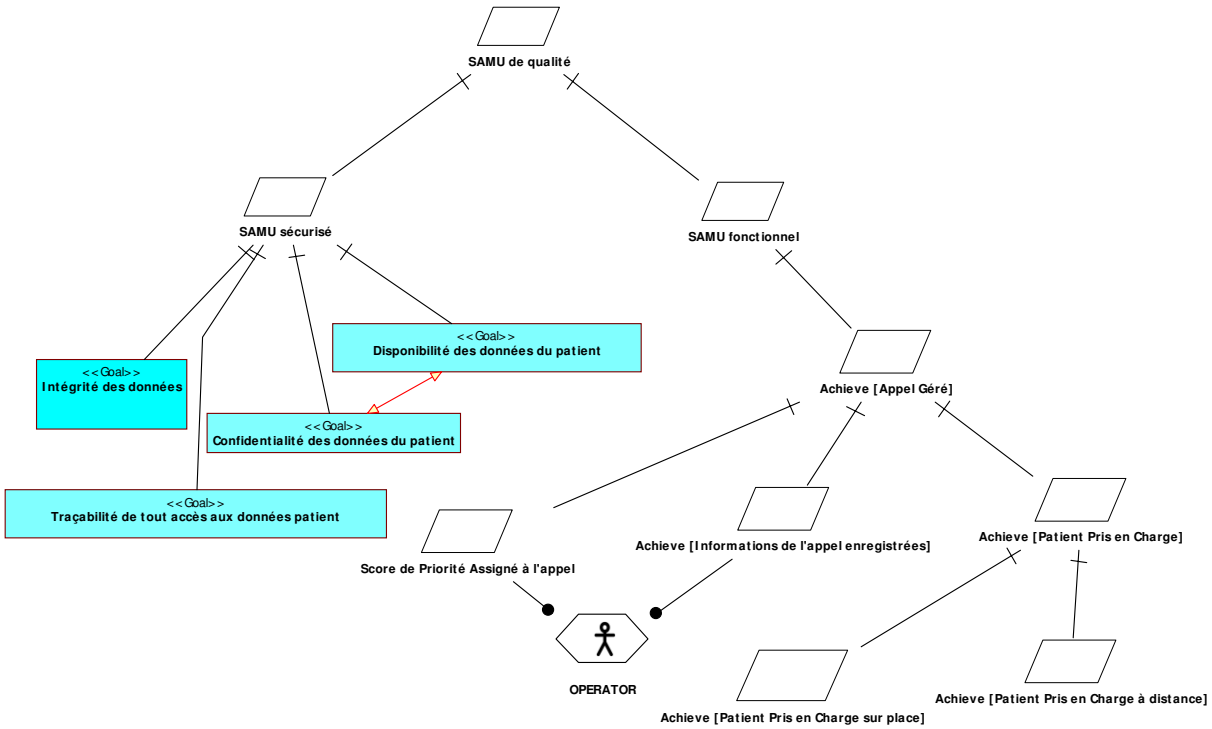


FIGURE 4.5 – The most abstract goals of the hierarchy, including security and functional goals

4.3.1 Construction of an agent hierarchy

The identification of actors plays a crucial role in both RBAC and KAOS. In KAOS, it selects the stakeholders which interact with the system. Reasoning on each of them helps to elicit the goals of interest for this agent. In the case of our security application, one can also review each of these agents and question whether he has some interest in breaking security rules and so become an attacker.

In this case study, our discussions with the representatives of IFREMMONT (who also provided the class diagrams and use cases) helped us identify the agents of Fig. 4.3. Please note that these focus on human agents, and don't include the system or software to develop (Res@mu).

It is also interesting to notice that patients are not actors in this system. Actually, they play a passive role and don't interact directly with the system. Each of their interactions goes through a member of the medical organisation.

As already mentioned, we felt the need for inheritance relations in this diagram. This is consistent with the fact that RBAC defines a hierarchy of roles. It must also be noted that we felt the need for multiple inheritance since there is a double partitioning of the main agents : those located in the call center vs those in direct contact with the patient, and the doctors and non-doctors.

4.3.2 Identification of use cases related to management acts

In order to identify the hierarchy of functional goals, we exploited the structure of use cases. As already mentioned, the initial UML diagrams include more than 100 use cases, and most of them are structured hierarchically. Fig. 4.6 gives a sample of these diagrams. The full diagram corresponding to the use cases linked to management acts is given in Fig. 4.9. These use cases express that there are two ways to take care of a patient : in-place and remotely. We omit the details of in-place operations and only detail remote care, which includes three cases : medical advice, prescription and instruction. Both in-place and remote operations must be validated.

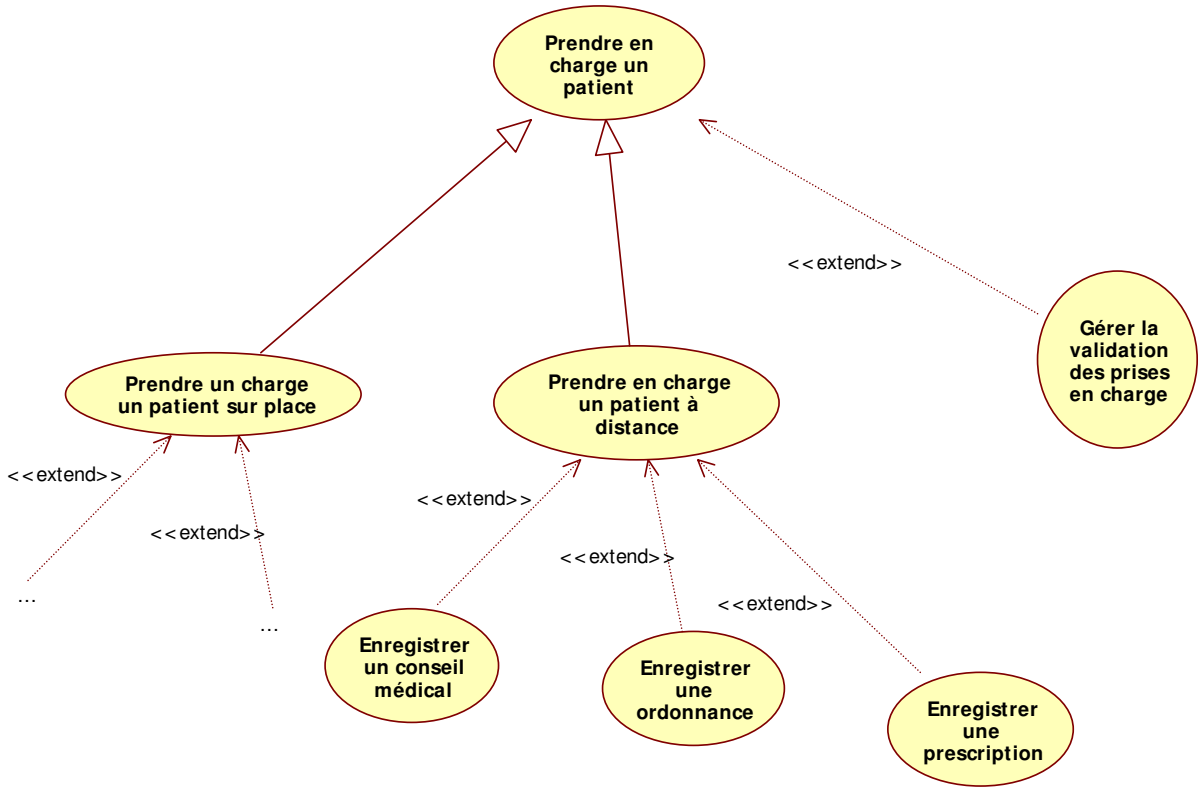


FIGURE 4.6 – Use cases related to the remote care of patients

4.3.3 Construction of a KAOS functional goal hierarchy

Use cases correspond to functionalities of the target system. In KAOS, they are close to goal operationalisation. So it makes sense to use them to identify the functional goals of our system. In this case study, we exploited the use case hierarchy to build our goal hierarchy.

The structure of these use cases has inspired the goal structure proposed in Fig. 4.4. In the goal diagram, prescriptions and instructions have been grouped in a single goal, because they share the common characteristic that they must be performed by a doctor, and because we did not feel the need to further distinguish between these for our security analysis purposes. Also, validation has been included as a sub-goal of the remote care. In the full diagram (Fig. 4.10), it is also linked to in-place care.

4.3.4 Identification of security goals linked to the data to protect

The security goals are first associated to ACIT properties. They are non-functional goals which apply to large parts of the system.

Here, we decided that each ACIT properties makes sense with respect to management acts :

- Availability : the medical data must be available to all members of the teams involved in emergency operations linked to the patient. This means that the information system must grant access to these data for all these personal. This availability remains after the emergency mission is closed to enable feedback for all the emergency personal on how the whole mission ended.
- Confidentiality : the medical data are confidential information, and may not be disclosed to actors not involved in the emergency operations linked to the patient.
- Integrity : it must be ensured that original data is not corrupted when transmitted or copied,

and not lost. Although it seems that it is only possible to add information to the system, some integrity properties remain. First, it must be possible to modify incorrect input, although this is not clearly supported in the use cases. Also, it appeared that ensuring that the right person does the validation is such an integrity issue.

– Traceability : every access to medical data, both for consulting and modifying should be logged.

These security goals appear on the KAOS diagram (Fig. 4.5, Fig. 4.10 or 4.11). The diagram also expresses that availability and confidentiality may be in conflict. Obviously, too strict confidentiality rules may prevent the rescue teams from accessing the necessary information. Conversely, too much availability may lead to disclose information to non-authorized actors.

Although the identification of these ACIT properties led to many discussions, the result is poorly captured by the KAOS diagrams at this stage. Security properties only appear as four short goals in the top of the hierarchy. Still these goals motivate the whole security policy, but give a poor explanation of the details. In other words, although this phase of the process led to substantial work, we probably need a better way to express and detail its results.

One of the results of these discussions was that a potential security hole may appear in the way emergency teams are built, and subsequently modified. Since access is granted to all members of the emergency team, one way to access medical data is to join the team. Care must thus be taken to make sure that nobody joins the team after the mission is completed (actually, the team is dedicated a single mission), and nobody joins the team during the mission without explicit authorisation from an authorized stakeholder, i.e. the regulator. This is the reason why, the goal "Equipe modifiée" appears in the KAOS hierarchy in Fig. 4.10 or 4.11.

4.3.5 Identification of functional goals linked to the protected data protected

The functional goals linked to "Management Act" appear in Fig. 4.10. In the restricted scope of Fig. 4.4, all lower level goals are concerned by these data.

For each of these goals, security must be enforced by several additional checks or actions, which will take the form of functional subgoals, refining the concerned functional goal. For example, Fig. 4.7 shows how the validation of a medical act corresponds to two subgoals : the explicit validation by the team member who did the act, and the verification by the software system that the person performing the validation was actually authorized to do so. This goal ("valideur autorisé") appears as a subgoal of both the functional goal ("acte de soin ou Prescription ou Ordonnance validé") and the non-functional goal "Intégrité des données".

4.3.6 Expression of RBAC rules which enforce security goals in the context of each functional goal

The next step is to express the RBAC rules in the class diagram. Fig. 4.12 gives the resulting class diagram for management acts[3]. The diagram includes the class Management Act, and the roles who may try to access it. These roles are the agents related to the goals directly linked to Management Act in Fig. 4.11. The model also includes agent "User", involved in the negative rules (interdiction) which apply by default.

Besides class Management Act, there is a need to represent subclass Medical Advice, because some different permissions apply to that class (PARMs have the right to access Medical Advices).

Permissions expressed on class Management Act apply to read and modification operations. Creation and deletion of Management Acts will presumably take place through the call of methods in classes Patient and PreHospital Actor which have a composition relation with Mana-

3. Actually, it should include additional rules for prescriptions and instructions.

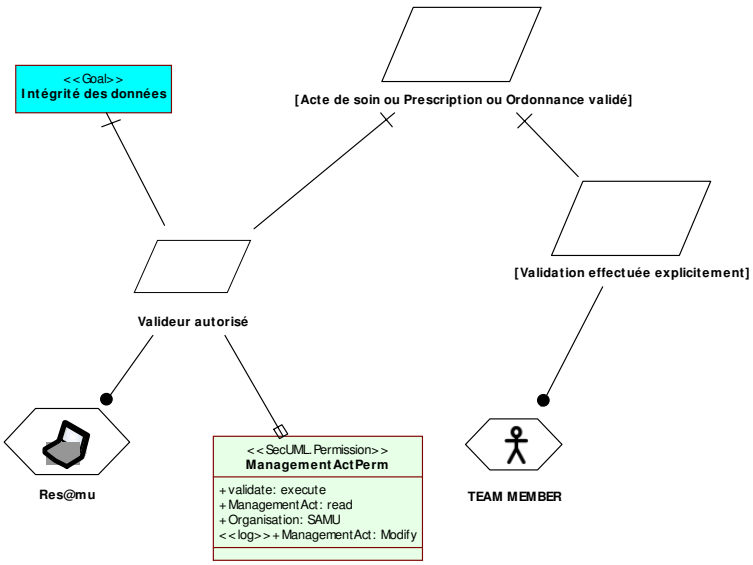


FIGURE 4.7 – From security goals to RBAC permissions

gement Act. Therefore these additional classes appear in the diagram.

At this stage, I don't detail the permissions expressed in this diagram ; this will probably be done in a future document, when the syntax of this diagram will have been better defined.

To complete this step, links must be established between permissions and the goals that they fulfill. For example, Fig. 4.7 links the goal "valideur autorisé" to the RBAC rule "ManagementActPerm" (to be more precise, it links it to the first element of the rule "validate : execute").

Another interesting point to discuss is how to relate actors to relevant classes in the diagram. For example, team members are pre-hospital actors, and it might be useful to express this link to be able to express some OCL constraints on the RBAC rules. For example, from the team member, one should be able to find out which team he belongs to and which patients were handled by this team. This will probably require to make a link between the definition of users in the RBAC model and the identification data stored in the functional data model.

4.3.7 Check of every relevant functional goal

The last step of our approach is to systematically review each functional goal linked to Management Act, and verify that the associated permissions are sufficient to carry out the goal.

For example, let us consider goal "Medical advice given" and the rules of Fig. 4.8. This goal can be achieved by a PARM or the regulator, who is a doctor. It only involves subclass Medical Advice of Management Act. It requires to be able to create a medical advice object, and once created, there is no possibility to modify it because it is instantly validated. The only remaining right for regulators and PARM is to read it. One can easily check that two RBAC rules are expressed for both actors. One of these rules is a read permission on Medical Advice, the other one is a permission to create such a Medical Advice for a given patient.

Each goal related to Management Act must be checked against the RBAC rules to ensure that the goal can be satisfied. In a later verification or validation activity, it will mean that a proof obligation may be expressed to check that the goal can be fulfilled (maybe in given circumstances), and that at least one test case should be associated to the goal to demonstrate that the goal can be fulfilled.

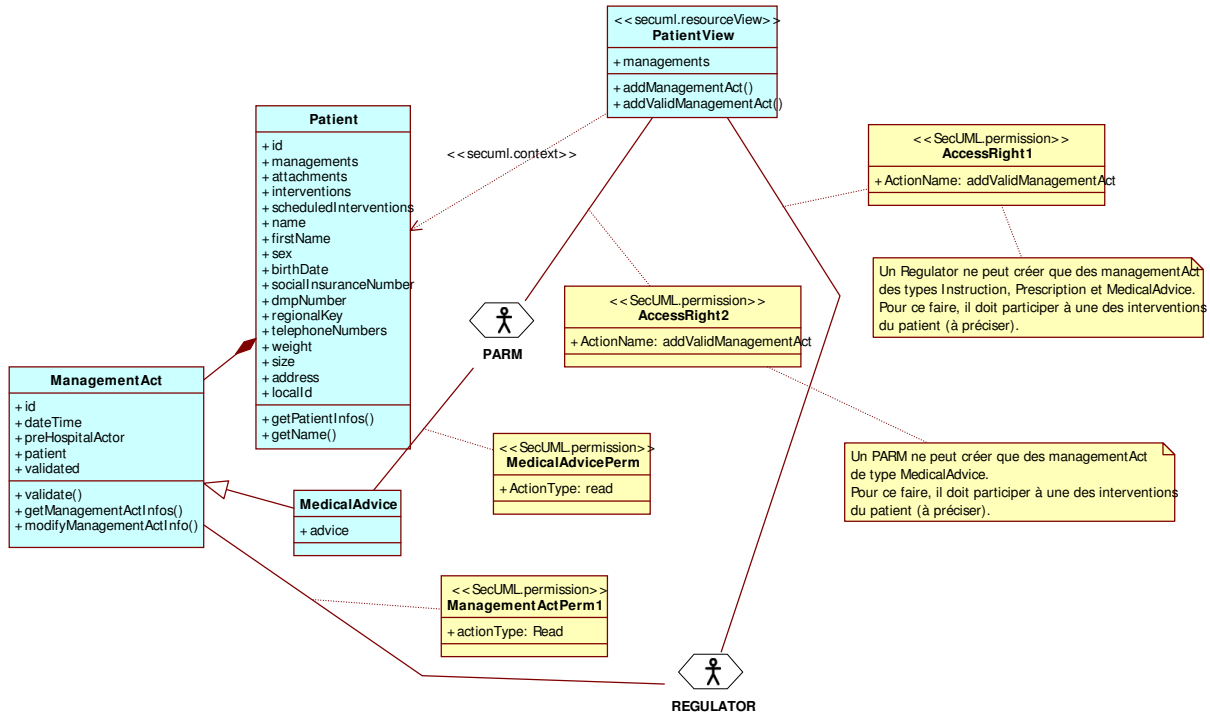


FIGURE 4.8 – The RBAC rules related to Medical Advice

4.4 Conclusion

This case study shows how a class diagram, initially provided with a set of use cases, can be completed by relevant RBAC rules.

From this case study, it appears that valuable information can be extracted from the initial UML diagrams (class diagram and use cases) which express only the functional aspects of the problem. Still, security properties are absent from these description. In our case study, they were first elicited from an extensive discussion with IFREMMONT. This discussion was mainly guided by the need to identify the relevant actors, and the relevant ACIT properties.

Another important choice is the use of KAOS diagrams. Although KAOS diagrams don't appear as mandatory in our approach, they have the nice feature that they can gather all important notions in a single diagram : functional goals, security properties (non-functional goals), actors, data (including RBAC permissions), and even operations or use cases. Although the construction of KAOS diagrams asks for supplementary efforts, it brings the potential benefit of this integration of all concepts, and allows the traceability between goals and RBAC rules. This case study only sketches this aspect, and future work is probably needed to explore and formalize it further.

Finally, an important step lies in the validation of the RBAC rules. Here we adopted a validation approach which made sure that each functional goal could be reached in the presence of security rules. Other validations are presumably needed, e.g. to evaluate the effectiveness of interdiction rules. It is also interesting to study the impact of integrity properties on RBAC rules. Also, traceability was not taken into account by our RBAC rules, and considered as a standard service of the target architecture.

Another analysis can be led on the KAOS model : the systematic identification of obstacles for every goal (functional or non-functional). Obstacles correspond either to hazards or to attacks. In the case of attacks, they are led by malicious actors. In section 4.2.2, we mentioned that the actor model could be studied in order to identify potential malicious actors. Further work should

be led to identify such actors and their corresponding attacks.

Acknowledgments This work was sponsored by the Selkis project : A development method of secure health care networks information systems : from requirements engineering to implementation (ANR-08-SEGI-018).

4.5 The other diagrams

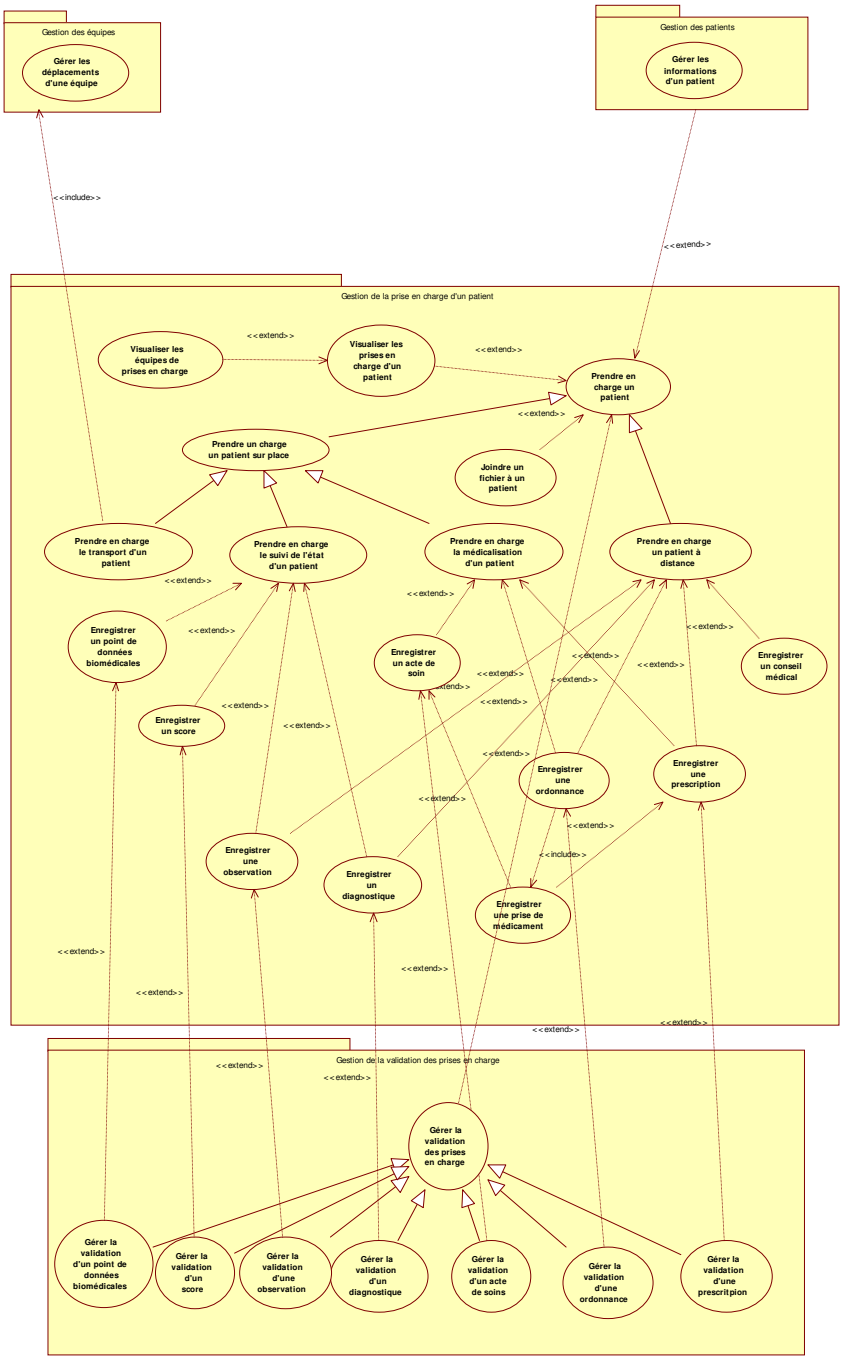


FIGURE 4.9 – The use cases related to management acts

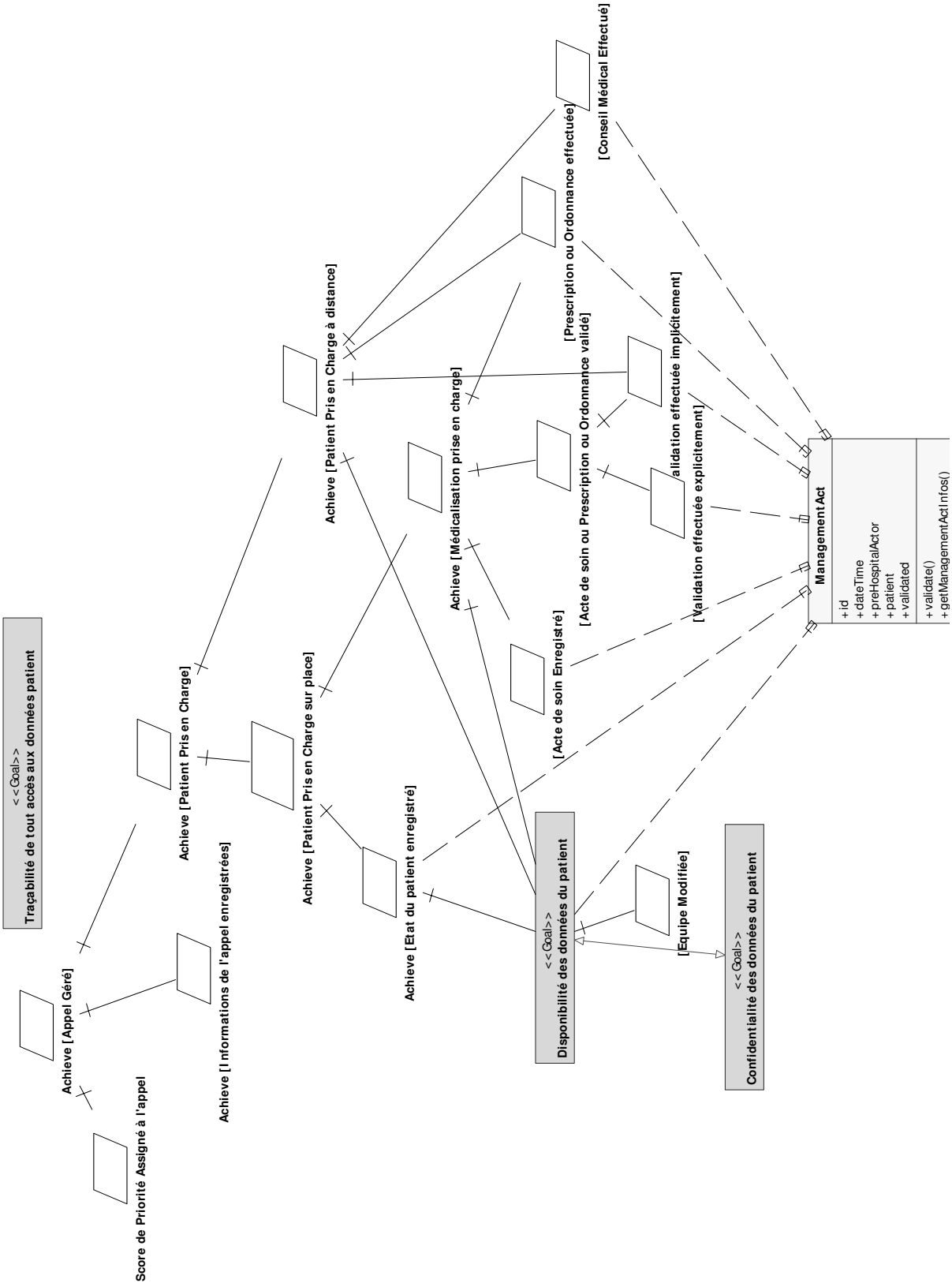


FIGURE 4.10 – The goals related to management acts (preliminary version)

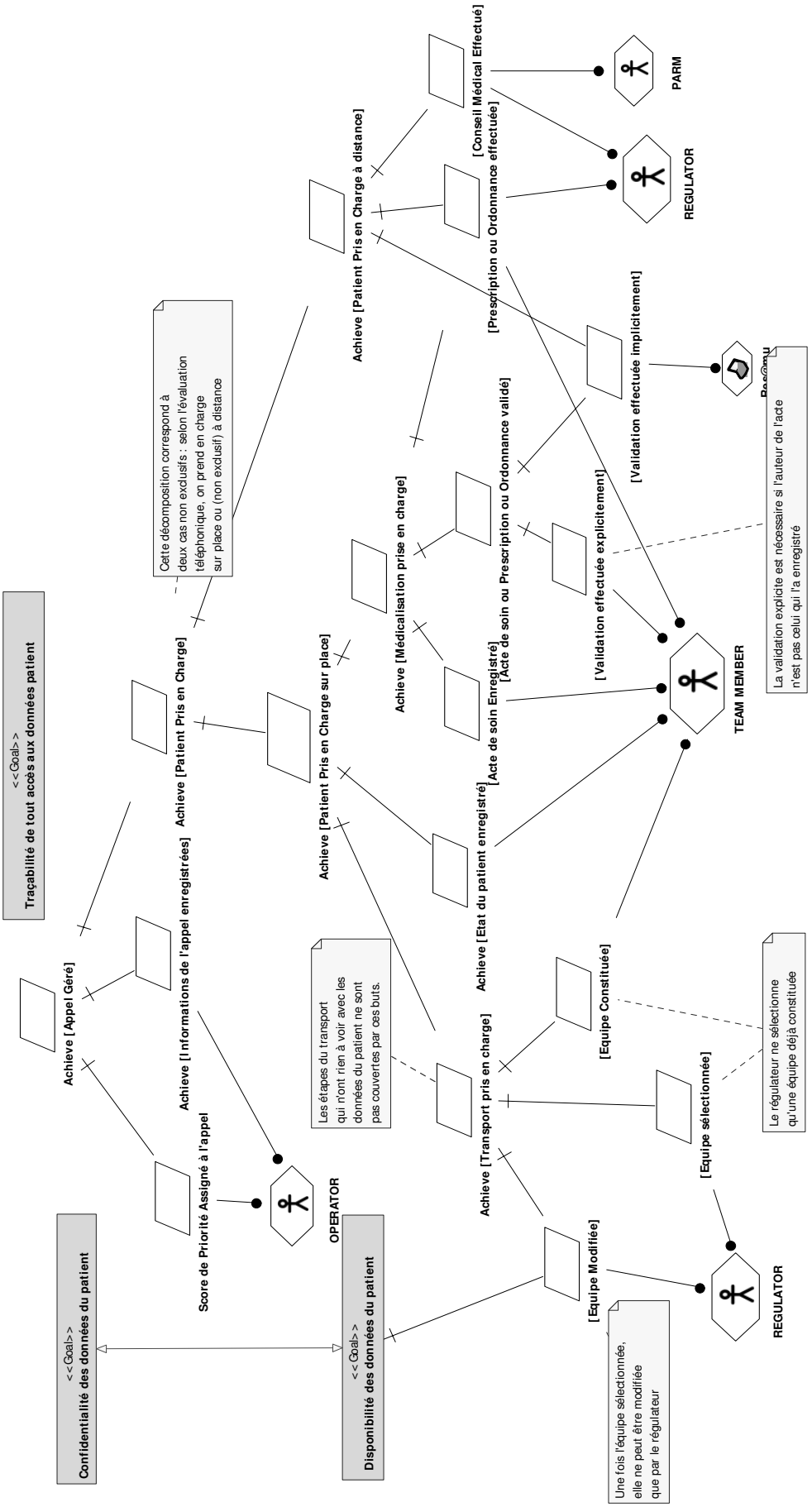


FIGURE 4.11 – Goals and actors related to management acts (preliminary version)

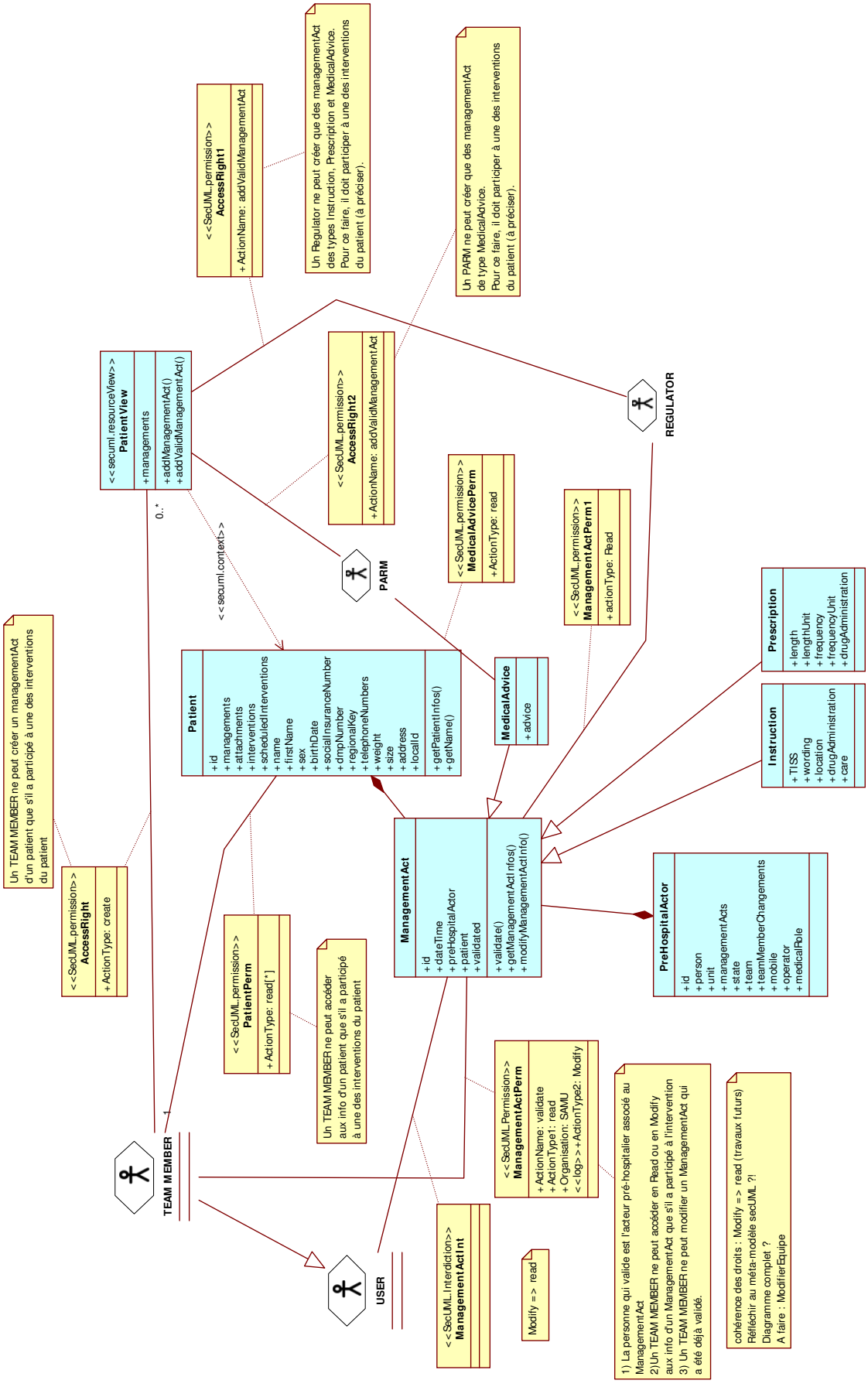


FIGURE 4.12 – RBAC rules integrated into the class diagram (preliminary version)

Bibliographie

[1] Role based access control. In *15th National Computer Security Conference*, pages 554–563, 1992.

[2] Axel van Lamsweerde. *Requirements Engineering : From System Goals to UML Models to Software Specifications*. Wiley, january 2009.

Chapitre 5

Présentation du modèle KAOS

Dans ce chapitre, nous décrivons le résultat de notre démarche d'identification des besoins de sécurité. Ces besoins sont présentés dans une hiérarchie de buts KAOS, liés à des règles RBAC. Ces diagrammes ont été préparés avec Star UML [1] et utilisent l'extension RE-Tools [2]

5.1 But de plus haut niveau : SAMU de qualité

Le premier diagramme (Fig. 5.1) décrit le but de plus haut niveau dans notre hiérarchie. Ce but a été nommé "SAMU de qualité". Ce but se décline en deux sous-buts : un but fonctionnel, "SAMU fonctionnel" (Sect. 5.3) et un but non fonctionnel, "SAMU sécurisé" (Sect. 5.2). Dans ce modèle, nous adoptons une syntaxe non-standard pour distinguer les buts fonctionnels des buts non-fonctionnels.

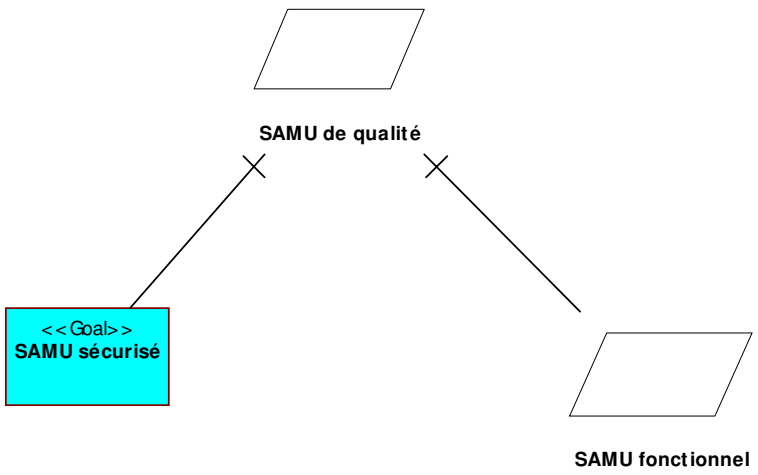


FIGURE 5.1 – Raffinement du but "SAMU de Qualité"

1. http://staruml.sourceforge.net
2. http://www.utdallas.edu/~supakkul/tools/RE-Tools/index.htm

5.2 Buts non-fonctionnels : SAMU sécurisé

La hiérarchie des buts non-fonctionnels est présentée à la Fig. 5.2. La décomposition du but "SAMU sécurisé" exprime que celui-ci contient les quatre propriétés ACIT : Availability (disponibilité), Confidentiality (confidentialité), Integrity (Intégrité) et Traceability (Traçabilité). Une flèche indique le conflit potentiel entre la disponibilité et la confidentialité. Il s'agira donc d'identifier un juste compromis pour satisfaire ces deux buts.

Parmi ces quatre buts, nous ferons l'hypothèse que la traçabilité est garantie par un mécanisme sous-jacent à la gestion des données. Il sera donc inutile de mettre en oeuvre la traçabilité par des règles de notre politique RBAC, ou par des buts fonctionnels associés. Les trois autres propriétés se traduisent généralement par des buts fonctionnels qui mettent en oeuvre la sécurité et sont associés à des règles RBAC. Une règle RBAC fait exception. Il s'agit de la règle "ManagementActInt" qui est directement rattachée à l'exigence de confidentialité.

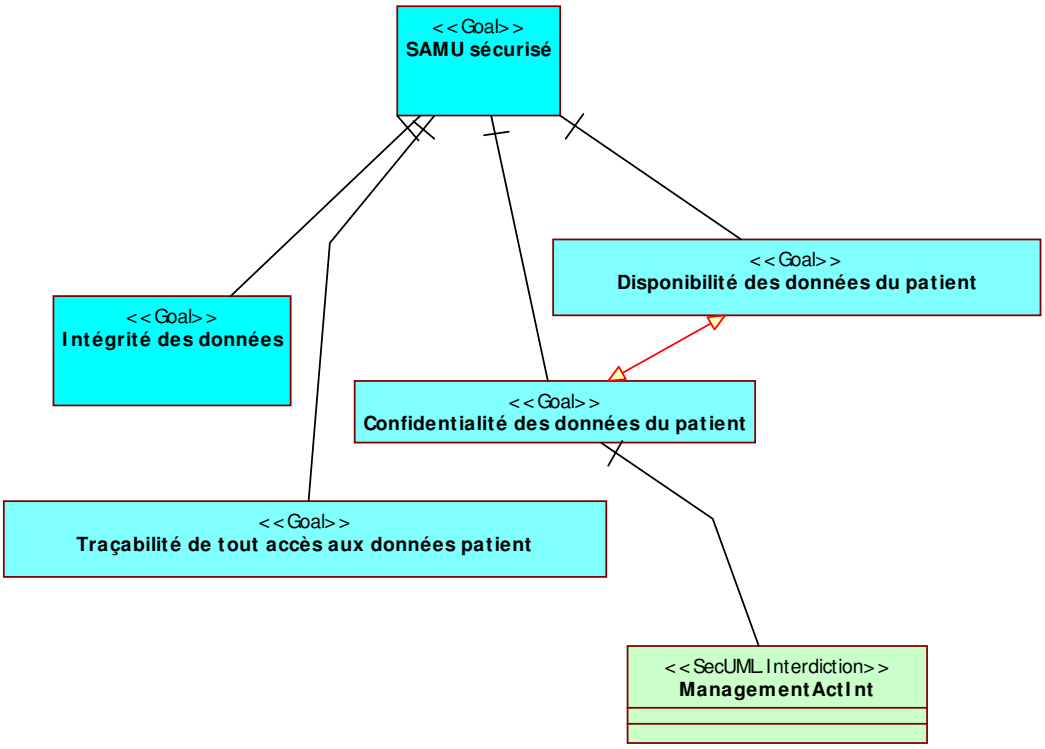


FIGURE 5.2 – But "SAMU sécurisé"

5.2.1 Règle "ManagementActInt"

Cette règle, présentée à la figure 5.3, exprime la règle d'accès par défaut à la classe ManagementAct : par défaut un utilisateur du système Res@mu n'a aucun droit d'accès à ManagementAct. Comme tous les utilisateurs du système spécialisent USER, ils héritent tous de cette interdiction.

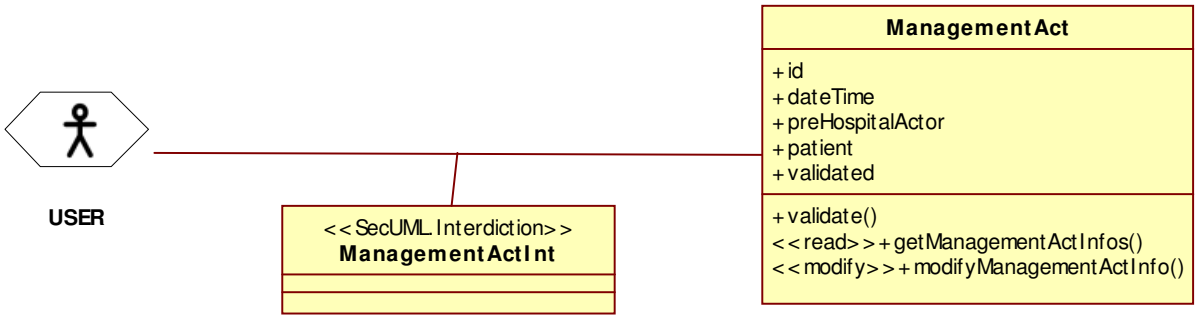


FIGURE 5.3 – Règle "ManagementActInt"

5.3 Buts qui définissent un SAMU fonctionnel

Les buts fonctionnels de plus haut niveau sont présentés à la Fig. 5.4. Cette figure est volontairement incomplète car elle ne présente que les buts de haut niveau liés à Management Act. Dans notre cas, il s'agit d'un seul but "Achieve[Appel Géré]". Dans une analyse non axée sur la sécurité de notre cible, d'autres buts apparaîtraient à ce niveau pour décrire d'autres aspects du SAMU : gestion des moyens, demandes d'aide, interventions, stocks, rapports,... Ces autres buts fonctionnels apparaissent dans les use cases de la modélisation fonctionnelle donnée au chapitre **??**.

Le but "Achieve[Appel Géré]" est raffiné en trois sous-buts. Les deux premiers sont accomplis par l'opérateur qui prend l'appel : l'appel se voit attribuer un score de priorité (but "Score de Priorité Assigné à l'appel"), par exemple en fonction de sa provenance (par exemple, un appel relayé d'un opérateur des pompiers), et, une fois que l'opérateur prend l'appel, il doit collecter diverses informations factuelles (but "Achieve [Informations de l'appel enregistrées]") avant de passer l'appel à un PARM ou un médecin régulateur.

Le but "Achieve [Patient Pris en Charge]" correspond à la prise en charge médicale de l'appel. Il est détaillé à la section 5.4.

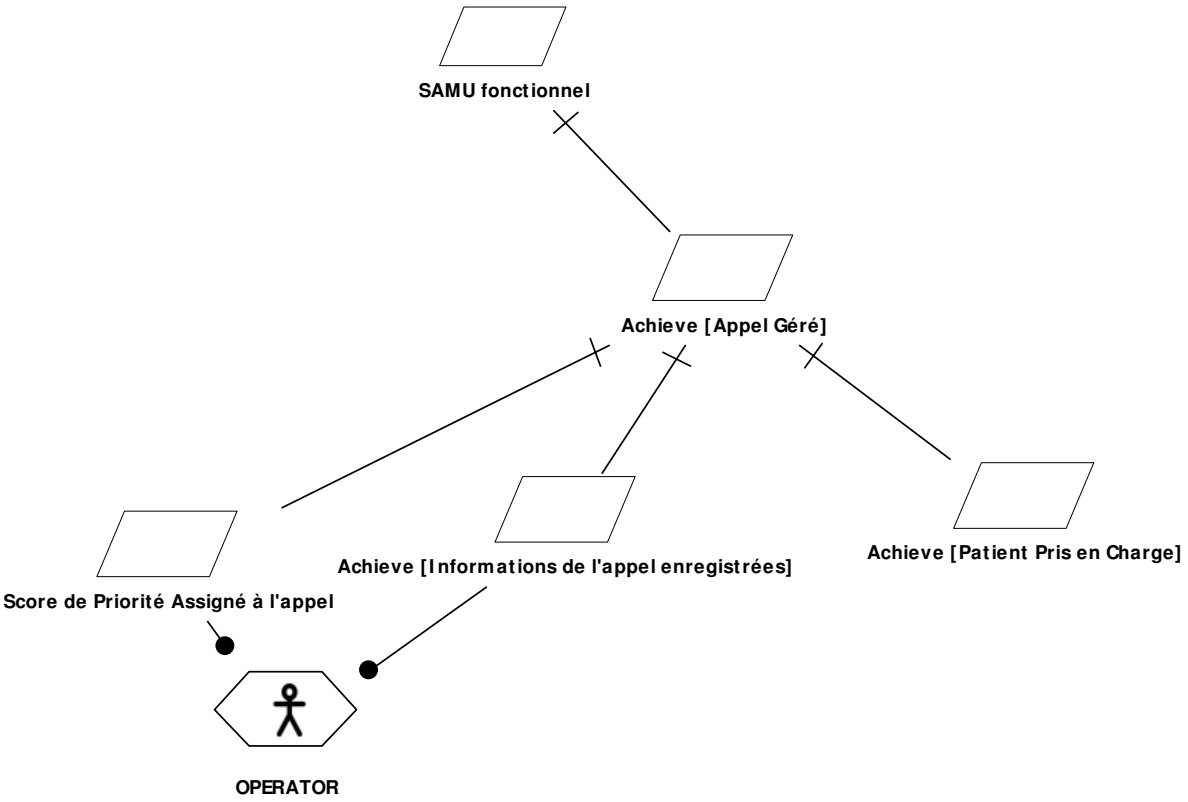


FIGURE 5.4 – But "SAMU fonctionnel"

5.4 Prise en charge du patient

La prise en charge du patient peut prendre deux formes : prise en charge sur place (but “Achieve [Patient Pris en Charge sur place]”,Sect. 5.7) ou à distance, par téléphone (but “Achieve [Patient Pris en Charge à distance]”,Sect. 5.6). Dans tous les cas, la prise en charge du patient comprend la consultation du dossier médical par les personnes concernées et autorisées (But “Achieve [Dossier Médical consulté]”, Sect. 5.5).

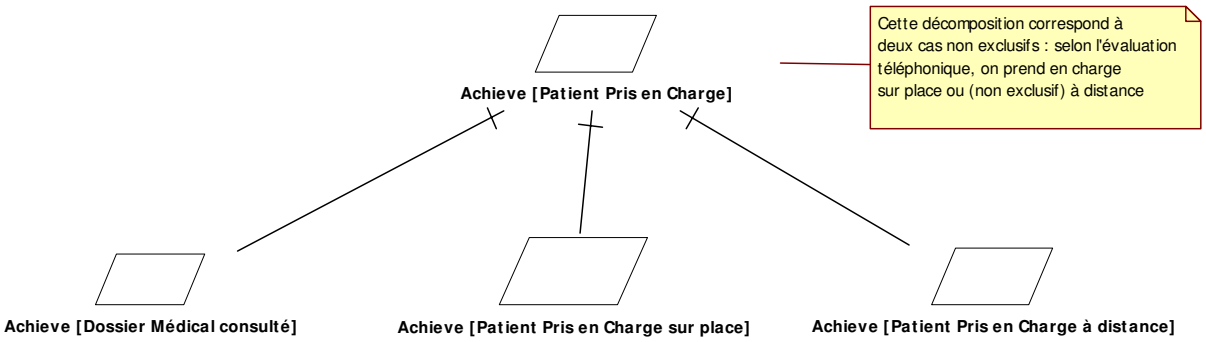


FIGURE 5.5 – But “Achieve [Patient Pris en Charge]”

5.5 Consultation du dossier médical

Pendant et après une intervention, toutes les équipes impliquées dans l'intervention ont la possibilité de consulter le dossier médical du patient. Pendant l'intervention, cela contribue à leur information sur l'état du patient et leur permet de prendre les bonnes décisions. Après l'intervention, cela contribue à la formation continue de ces personnels en leur permettant de passer en revue les actes médicaux qui ont été posés, et en leur donnant des informations sur l'évolution du patient après l'intervention. Ceci exprime essentiellement un besoin de disponibilité en lecture du dossier du patient.

Il existe également un besoin de confidentialité du dossier du patient. Ce besoin est satisfait de deux manières : d'une part, l'accès en consultation au dossier du patient n'est accordé qu'aux membres des équipes d'intervention concernées par ce patient, c'est-à-dire celles qui sont identifiées ci-dessus comme ayant un besoin de disponibilité en lecture de ce dossier. D'autre part, ces personnes qui ont accès au dossier du patient sont toutes liées par le secret médical. Cette propriété est exprimée comme une attente (expectation) en sous-but du but de confidentialité.

Le but "Achieve[Accès au dossier autorisé]" est un but fonctionnel qui met en place un contrôle d'accès au dossier. Ce but est directement lié au système informatique qui est responsable de sa réalisation. Il contribue à la confidentialité des données en ne donnant accès au dossier qu'aux personnes autorisées. Ce contrôle d'accès se base sur quatre règles du modèle RBAC : "PatientPerm", "ManagementActPerm" (Fig. 5.7), "MedicalAdvicePerm" et "ManagementActPerm1" (Fig. 5.8). Toutes ces règles comprennent une permission de type "Read" qui porte directement ou indirectement sur ManagementAct.

Une fois ce contrôle d'accès effectué, la consultation du dossier proprement dite peut avoir lieu (but "Achieve[Dossier Consulté]"). Cette consultation est réalisée par les trois types d'agents concernés : TEAM MEMBER, REGULATOR et PARM.

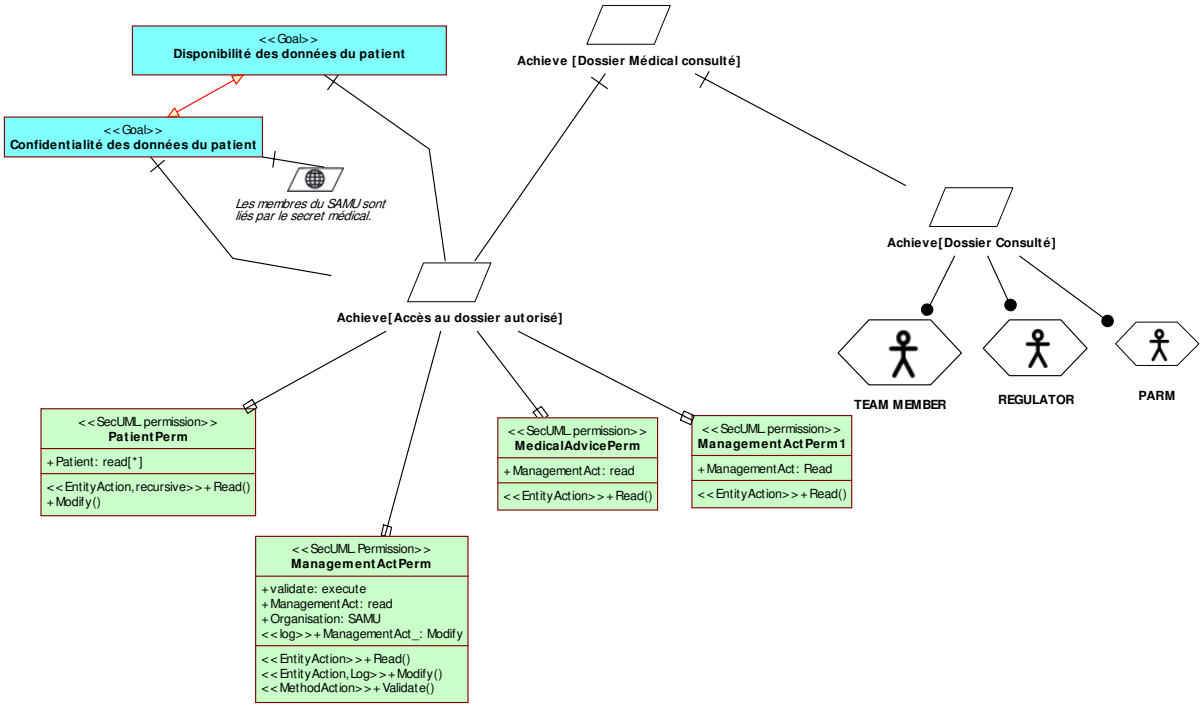


FIGURE 5.6 – But "Achieve [Dossier Médical consulté]"

5.5.1 Règles “PatientPerm” et “ManagementActPerm”

La Fig. 5.7 exprime les permissions accordées à TEAM MEMBER pour la consultation et la modification des Management Acts. La règle principale est la règle ManagementActPerm qui exprime trois types de permissions pour les TEAM MEMBERs sur la classe ManagementAct :

– Un droit en lecture (Read), qui correspond à toutes les méthodes stéréotypées par “read” dans ManagementAct (ici getManagementActInfos()). Ce droit est conditionné à une contrainte : “Un TEAM MEMBER ne peut accéder (en lecture, ecriture) aux informations d’un ManagementAct que s’il a participé à l’intervention”. Cette contrainte est également exprimée en OCL et s’applique à toutes les règles de ManagementActPerm.
– Un droit de modification (Modify), correspondant à la méthode modifyManagementActInfo() et limité par la contrainte : “Un TEAM MEMBER ne peut modifier un ManagementAct qui a été déjà validé”. Cette contrainte se combine à celle ci-dessus.
– Un droit de validation limité à la seule méthode validate() et la contrainte “La personne qui valide est l’acteur pré-hospitalier associé au ManagementAct”. Ce droit de validation est utilisé dans le cas de la validation explicite (Fig. 5.11).

La règle “PatientPerm” est plus expérimentale car elle inclut un droit en lecture récursif sur Patient. La signification de ce mot clé “recursive” est que le droit est accordé à la classe et à toutes les classes inclues dans celle-ci par un lien de composition. La deuxième règle donne la possibilité à un team member de modifier les informations administratives du patient, en fonction de la collecte des données effectuée sur place. Une contrainte limite cette possibilité de modification à la durée de l’intervention.

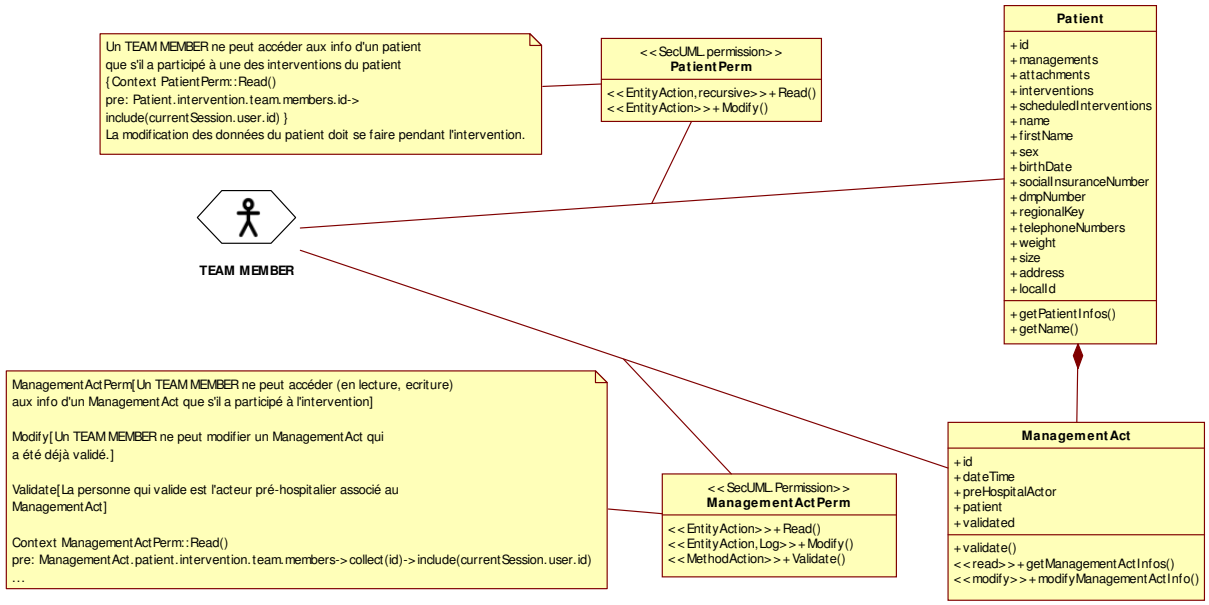


FIGURE 5.7 – Règles “PatientPerm” et “ManagementActPerm”

5.5.2 Règles “MedicalAdvicePerm” et “ManagementActPerm1”

Ces deux règles sont présentées à la Fig. 5.8. Elles traduisent la règle Read de “ManagementActPerm” pour les rôles REGULATOR et PARM : ces deux rôles ont un droit en lecture sur les données médicales des patients pour lesquels l’agent correspondant a participé à l’intervention.

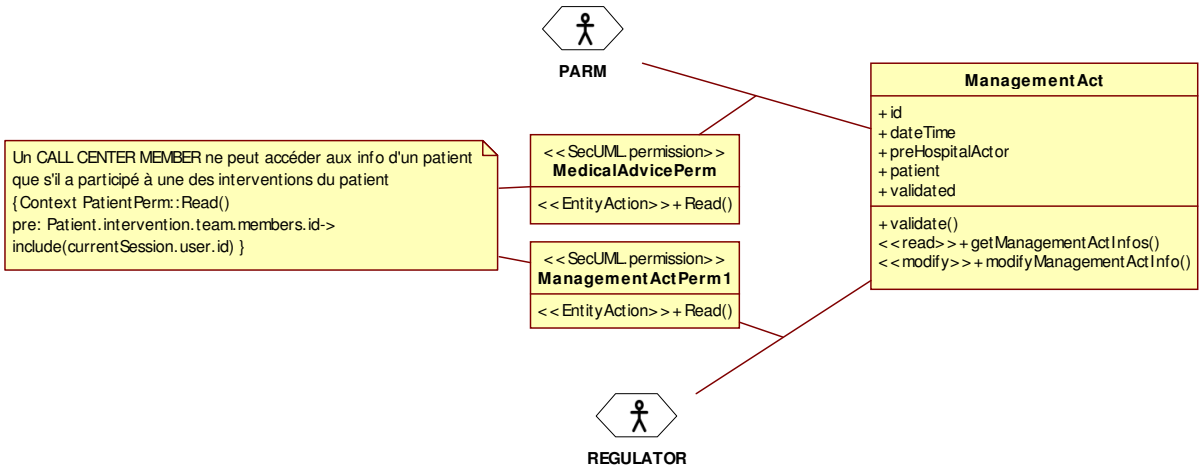


FIGURE 5.8 – Règles “MedicalAdvicePerm” et “ManagementActPerm1”

5.6 Prise en charge à distance

La Fig. 5.9 traite le cas de la prise en charge d'un patient à distance. Cela correspond au cas où les membres du call center (REGULATOR ou PARM) font des actes médicaux à distance. Ces actes médicaux peuvent prendre plusieurs formes :

– le conseil médical (But "Conseil Médical Effectué"), qui peut être donné par le PARM ou par le médecin ; ce conseil doit être guidé par le système informatique ce qui diminue fortement les risques d'un mauvais encodage.
– l'émission par le médecin d'une prescription ou d'une ordonnance qui sera envoyée au patient ou à un personnel médical proche du patient (cas d'une prescription) (But "Prescription ou Ordonnance effectuée").

Deux buts fonctionnels, réalisés par l'agent Res@mu et liés à la sécurité apparaissent dans ce diagramme :

– Le but "Achieve [Droit accordé pour ajouter un acte]" contribue à l'intégrité du système en vérifiant que la personne qui crée l'acte médical est autorisée à le faire. Ceci est mis en oeuvre par les deux règles RBAC "AccessRight1" et "AccessRight2" (Fig. 5.10). Il faut noter que la Fig. 5.11 ajoute une troisième règle "AccessRight" (Fig. 5.10)pour réaliser ce même but.
– Le but "Achieve[Validation effectuée implicitement]" effectue automatiquement la validation des actes médicaux créés par les personnels du Call Center. En effet, les risques d'erreur d'encodage sont très faibles et l'encodage est effectué par la personne responsable de l'acte. Il est inutile de demander à ces personnels une phase de validation explicite. Comme ce but fonctionnel est réalisé par l'agent logiciel Res@mu, il n'est pas lié à une règle de contrôle d'accès.

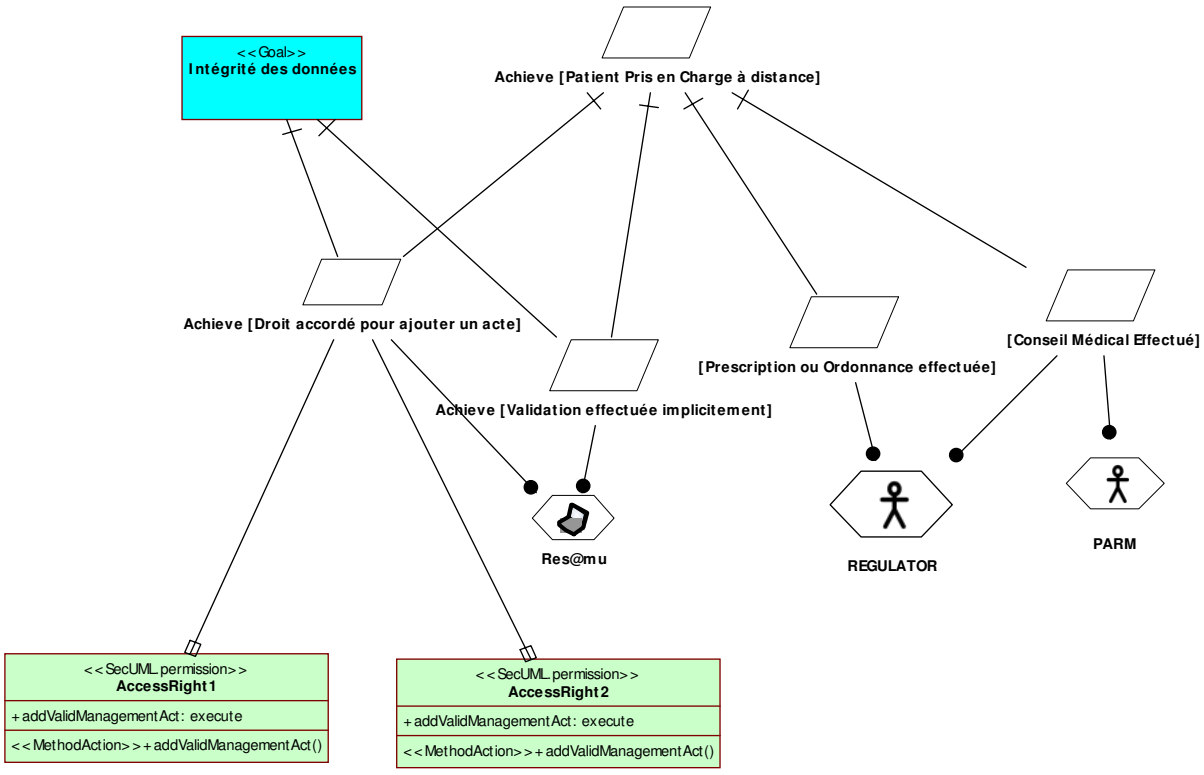


FIGURE 5.9 – Prise en charge d'un patient à distance

5.6.1 Règles “AccessRight1” et “AccessRight2”

Pour créer un acte médical, il faut invoquer une méthode de la classe Patient. Dans le cas de prise en charge distante, il s’agit de la méthode addValidManagementAct(), qui ajoute un tel acte et le valide automatiquement. Les règles “AccessRight1” et “AccessRight2” (Fig. 5.10) expriment que les rôles REGULATOR et PARM, qui correspondent aux membres du call center habilités à créer des actes médicaux, ont le droit d’invoquer la méthode addValidManagementAct.

Dans cette figure, une vue PatientView est extraite de Patient et limitée aux attributs et méthodes concernées par ces règles. Comme la même vue sera utilisée pour les règles de création liées à TEAM MEMBER (Fig. 5.12), elle inclut également la méthode AddManagementAct().

Deux contraintes, traduites partiellement en OCL, complètent ces règles. Elles expriment que les deux rôles concernés ne peuvent créer que certaines catégories d’actes médicaux et qu’ils doivent participer à une des interventions du patient pour pouvoir faire un tel ajout.

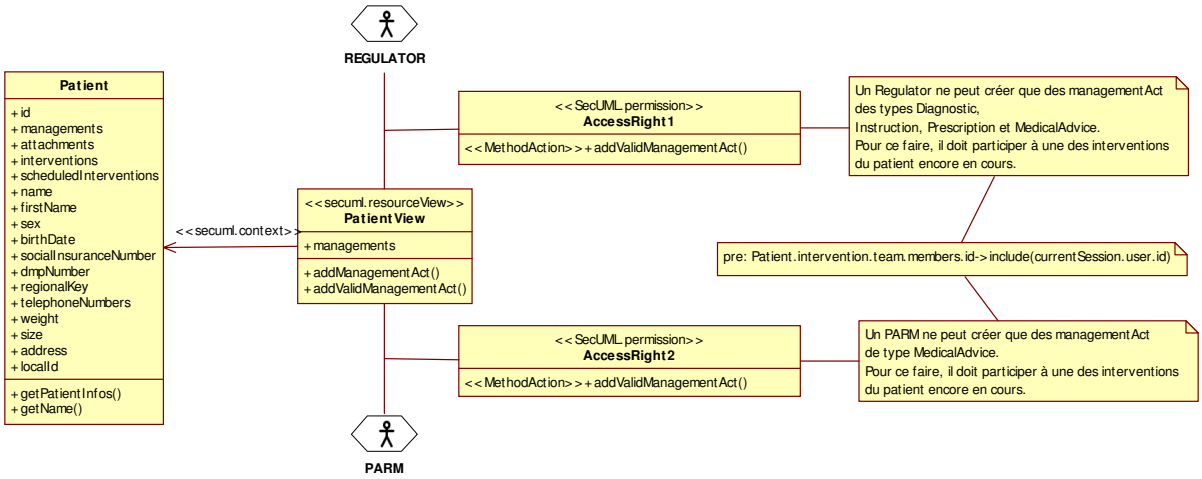


FIGURE 5.10 – Règles “AccessRight1” et “AccessRight2”

5.7 Prise en charge sur place

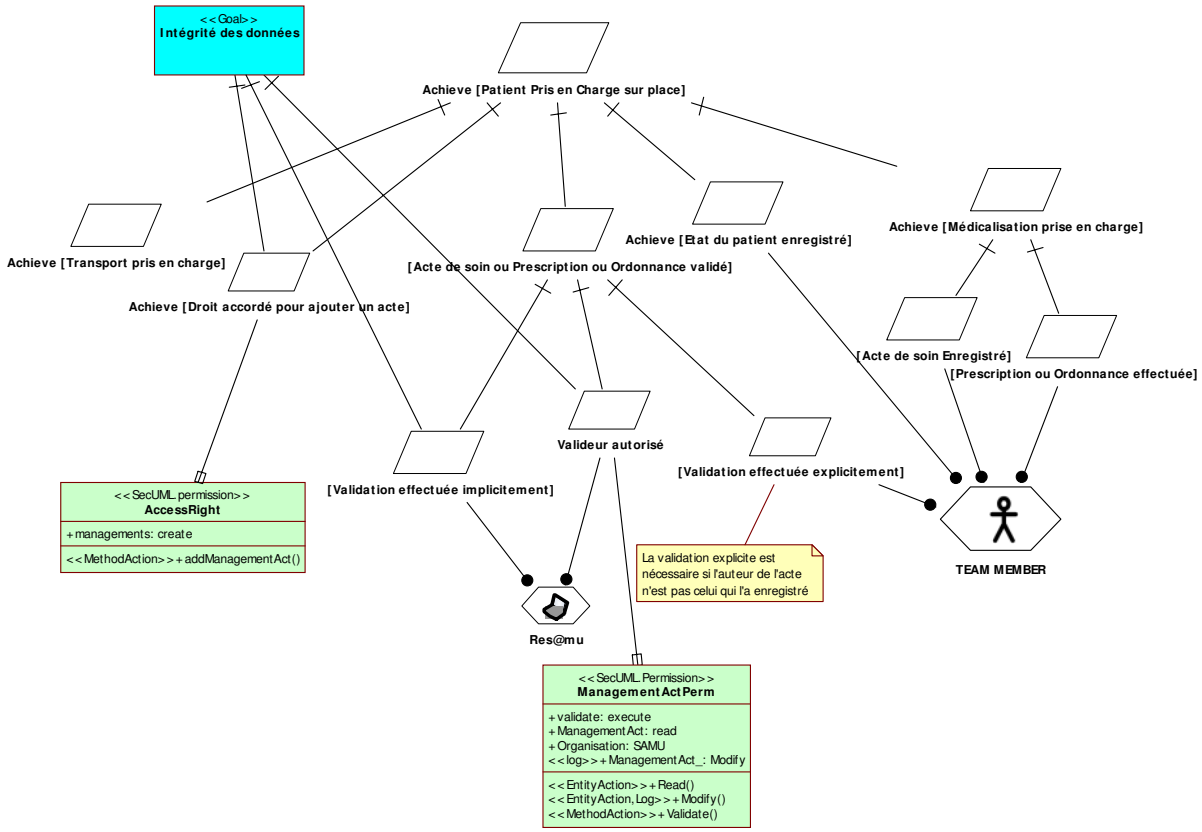


FIGURE 5.11 – Prise en charge d'un patient sur place

La Fig. 5.11 détaille l'ensemble des sous-buts associés à la prise en charge sur place.

Plusieurs types d'actes médicaux peuvent être effectués par les membres des équipes des secours (TEAM MEMBER) : l'enregistrement de l'état du patient (but "Achieve [Etat du patient enregistré]"), qui comprend divers types d'actes médicaux (observations, diagnostic,...), la prescription ou l'ordonnance (but "Prescription ou Ordonnance effectuée"), et la réalisation d'un soin ("Acte de soin Enregistré"). Ces deux derniers types d'actes correspondent à un but plus abstrait "Achieve [Médicalisation prise en charge]".

Comme dans le cas de la prise en charge à distance, deux buts fonctionnels, liés à la sécurité et plus précisément à l'intégrité, accompagnent ces enregistrements d'actes médicaux :

- Le but "Achieve [Droit accordé pour ajouter un acte]" vérifie que le personnel a le droit d'enregistrer un tel acte. Il est mis en oeuvre par la règle "AccessRight" et est effectué par le logiciel Res@mu.
- Le but "Acte de soin ou Prescription ou Ordonnance validé" correspond à la validation des actes médicaux. Cette validation peut être implicite, si la personne qui enregistre l'acte est celle qui en est responsable. Dans ce cas, la validation est effectuée directement par Res@mu. Dans le cas contraire, la validation doit être effectuée explicitement par le responsable (un TEAM MEMBER). Ce but "Validation effectuée explicitement", est précédée par le but "Valideur autorisé", effectué par Res@mu au travers de la règle validate de "ManagementActPerm" (Sect. 5.5.1, Fig. 5.7).

Un dernier but raffine le but de haut niveau "Achieve [Patient Pris en Charge sur place]". Il s'agit du but "Achieve [Transport pris en charge]" qui organise le transport du patient mais permet également de modifier la composition des équipes, et ainsi la liste des personnes ayant

accès au dossier (Sect. 5.8).

5.7.1 Règle “AccessRight”

Cette règle est la traduction pour les TEAM MEMBER de la règle de création d’un acte médical (voir Sect. 5.6.1, Fig. 5.10). Contrairement aux membres des call centers, les TEAM MEMBERs n’ont pas de restriction sur la nature des actes qu’ils peuvent créer.

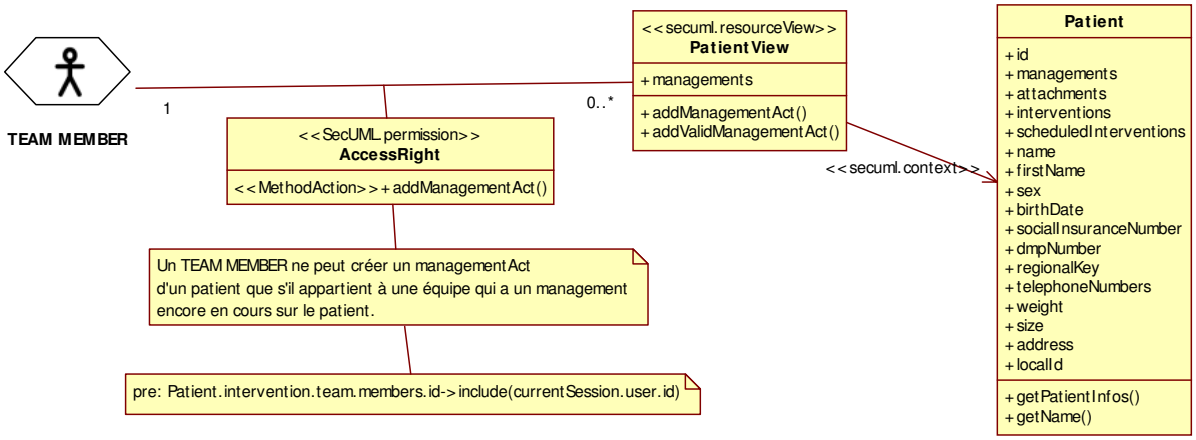


FIGURE 5.12 – Règle “AccessRight”

5.8 Constitution des équipes et organisation du transport

Le but “Achieve [Transport pris en charge]” est pris en considération dans cette étude parce qu'il pourrait mettre à mal la confidentialité des données du patient, via la modification de la composition des équipes. En effet, la confidentialité des données médicales est protégée en limitant leur accès aux membres des équipes d'intervention. Une façon de contourner cette règle est de modifier a posteriori la composition de ces équipes pur y ajouter un membre non autorisé. A cet effet, le but est décomposé en trois sous-buts qui décrivent de façon sommaire la constitution et la modification des équipes. Il ressort d'une réunion récente avec IFREMMONT que cette partie du diagramme doit être revisée car en réalité le processus est plus complexe (une équipe est constituée suite à une demande d'aide et elle peut être modifiée à l'initiative de ses membres). Par ailleurs, il faudrait définir une nouvelle cible de sécurité (la classe TEAM) pour sécuriser les opérations de constitution et surtout de modification des équipes.

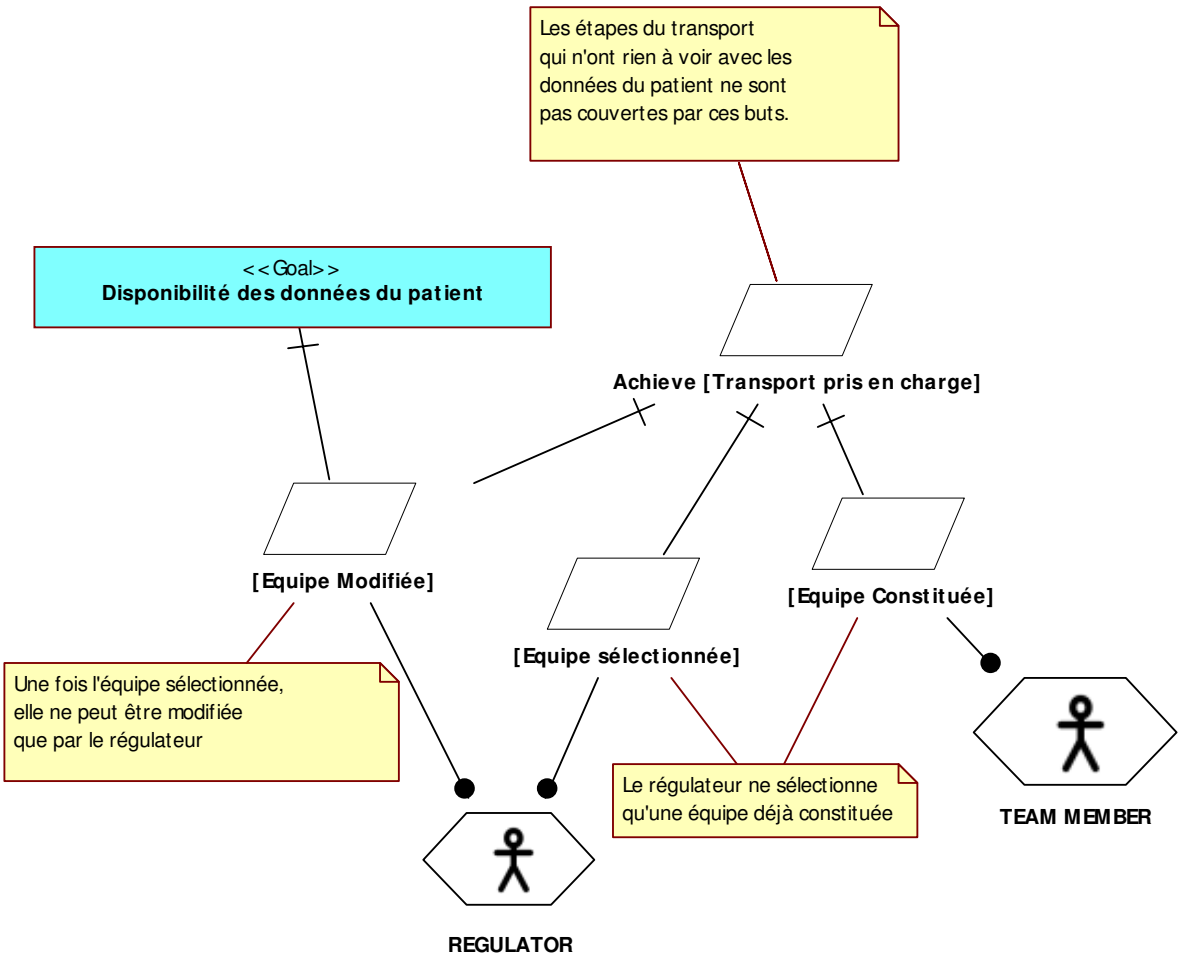


FIGURE 5.13 – Constitution des équipes et organisation du transport

5.9 Buts concernés par Management Act

Dans la Sect. 4.2.3, nous avons mis l'accent sur la possibilité d'exprimer des liens entre les buts KAOS et les données du diagramme de classes. Ceci est exploité dans notre méthode d'identification des besoins de sécurité (Sect. 4.3.5) pour identifier les buts fonctionnels liés à la cible de sécurité. Dans ce chapitre, nous présentons le résultat de notre démarche et non les étapes qui y ont mené. Cependant, pour être complet, nous donnons à la Fig. 5.14 l'ensemble des buts, fonctionnels ou non, concernés par la classe Management Act.

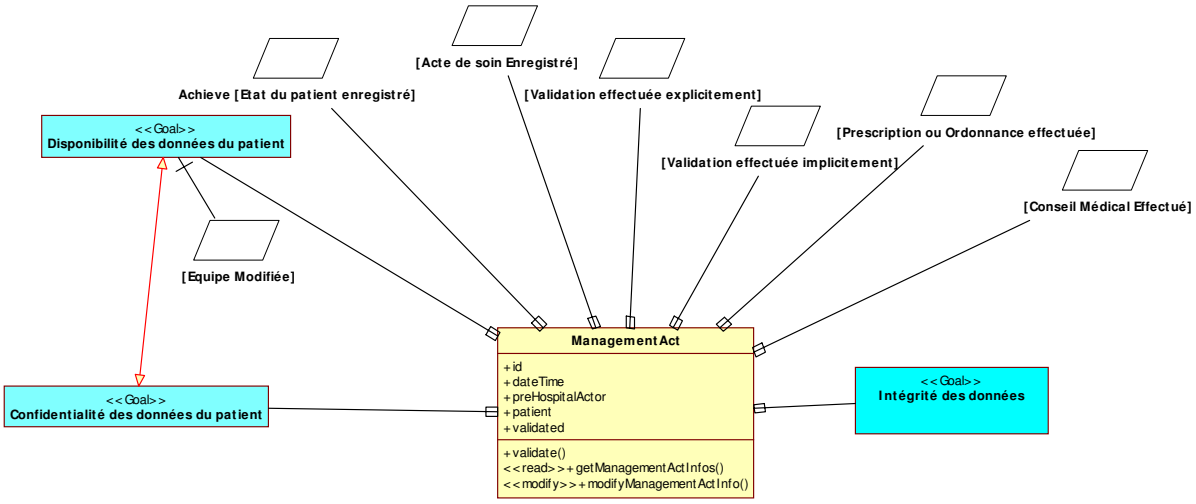


FIGURE 5.14 – Buts concernés par Management Act

5.10 Modèle RBAC résultant

La Fig. 5.15 reprend dans un seul diagramme l'ensemble des règles RBAC présentées dans cette étude de cas.

5.11 Conclusion

Ce chapitre a présenté le modèle KAOS utilisé pour raffiner les besoins de sécurité, exprimés au niveau ACIT vers une politique de contrôle d'accès exprimée par des règles RBAC.

Pour ce faire, le modèle KAOS fait l'objet d'une décomposition fonctionnelle, basée sur la structure des use cases. Les buts fonctionnels ayant accès à la cible de sécurité ont été complétés par des buts qui mettent en oeuvre la politique de contrôle d'accès. Ces buts, qui sont de nature fonctionnelle font le lien entre les règles de sécurité de haut niveau et leur mise en oeuvre par des règles RBAC.

Ces règles ont été présentées au fur et à mesure de leur utilisation dans les diagrammes. Elles sont conformes au méta-modèle défini dans la tâche WP2 du projet Selkis.

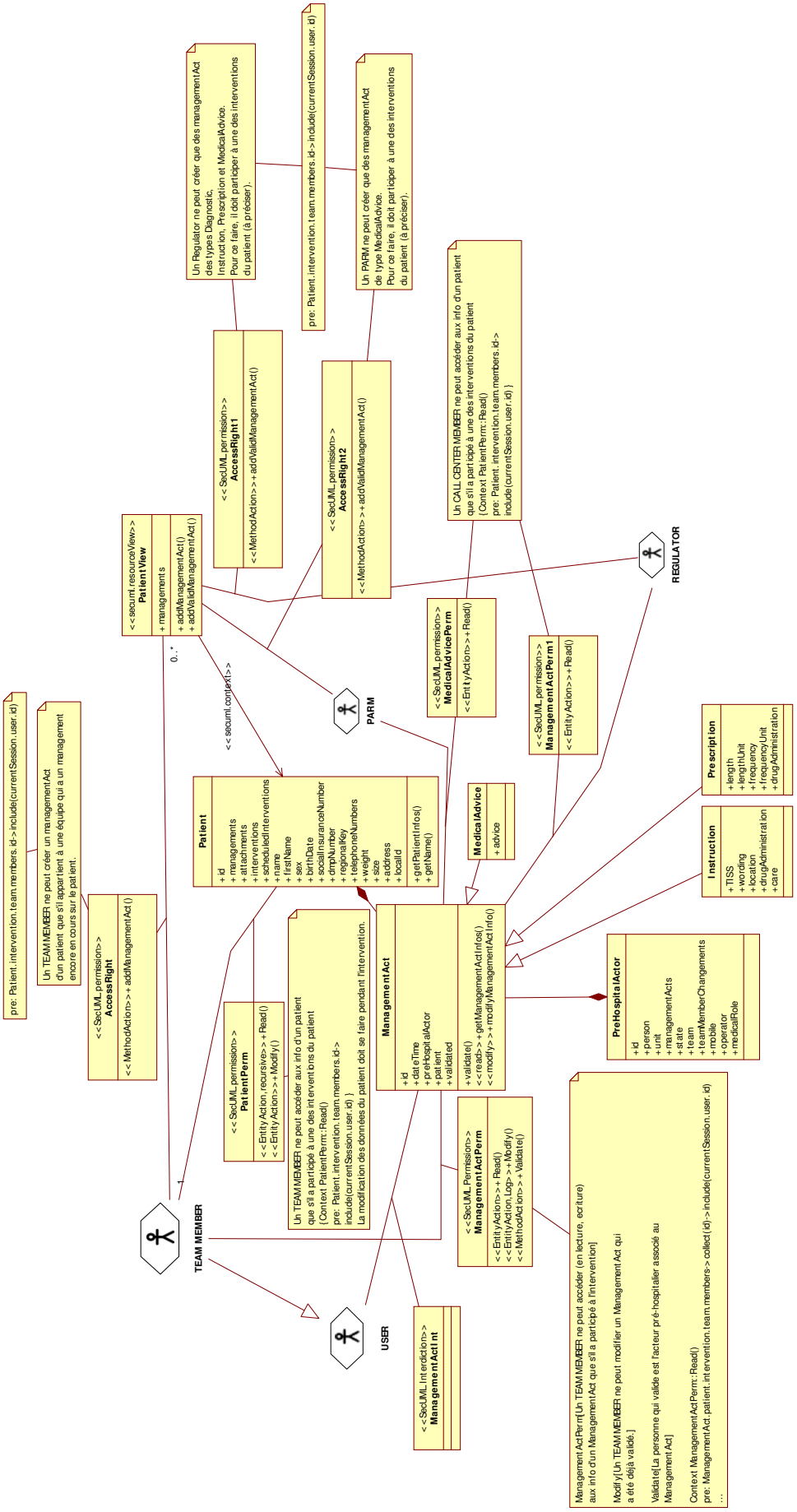


FIGURE 5.15 – Modèle RBAC de contrôle des accès à ManagementAct