

*Étude de cas : contrôle d'accès à un bâtiment*

On souhaite protéger un bâtiment en restreignant l'accès à certaines salles. Pour cela, l'ouverture de chacune des portes de ces salles est commandée par un lecteur de badges placé à proximité. Les badges qui permettent l'ouverture des portes ne sont délivrés qu'aux personnes qui doivent accéder aux locaux protégés dans l'exercice de leurs fonctions. Les droits d'accès sont alloués entre les groupes de personnes et les groupes de portes, de sorte qu'une personne ou une porte doit toujours être au moins dans un groupe (le sien).

Un groupe de portes peut contenir des portes dispersées dans tout le bâtiment. Une porte donnée ne peut appartenir qu'à un seul groupe de portes.

La même personne peut appartenir à plusieurs groupes, de sorte que ses droits d'accès correspondent à l'union des droits d'accès de chacun des groupes qui la contiennent.

La définition des droits d'accès est effectuée en décrivant pour chaque groupe de personnes les différents groupes de portes qui sont accessibles et sous quelle contrainte horaire. Les droits d'accès sont décrits dans un calendrier annuel qui décrit la situation semaine par semaine. Vu la faible variation des droits dans le temps, un calendrier peut être initialisé au moyen de semaines types qui décrivent une configuration de droits donnée. Le superviseur peut créer autant de semaines type qu'il le désire. Les changements apportés à une semaine sont automatiquement propagés dans tous les calendriers qui utilisent cette semaine type.

Le système de contrôle d'accès doit fonctionner de la manière la plus autonome possible. Un superviseur est responsable de la configuration initiale et de la mise à jour des différentes informations de définition des groupes de personnes et de portes. Un gardien dispose d'un écran de contrôle et est informé des tentatives de passage infructueuses. Les alarmes sont transmises en temps légèrement différé: la mise à jour de l'information sur l'écran de contrôle est effectuée toutes les minutes.

1. Décrire la vue des besoins (use case view) de ce système de contrôle d'accès. Cette analyse des besoins consiste à définir :
  - les acteurs de ce système.
  - le diagramme des cas d'utilisation du système.

- les principaux scénarios de chaque cas d'utilisation qui seront décrits par des diagrammes de séquence (point de vue temporel).
2. Décrire la vue logique (logical view) de ce système. Cette analyse du domaine consiste à définir :
- le diagramme des classes.
  - décrire les principaux scénarios par des diagrammes de collaboration (interactions entre objets d'un point de vue spatial). Il est bien évidemment possible de représenter les interactions entre objets par des diagrammes de séquence.