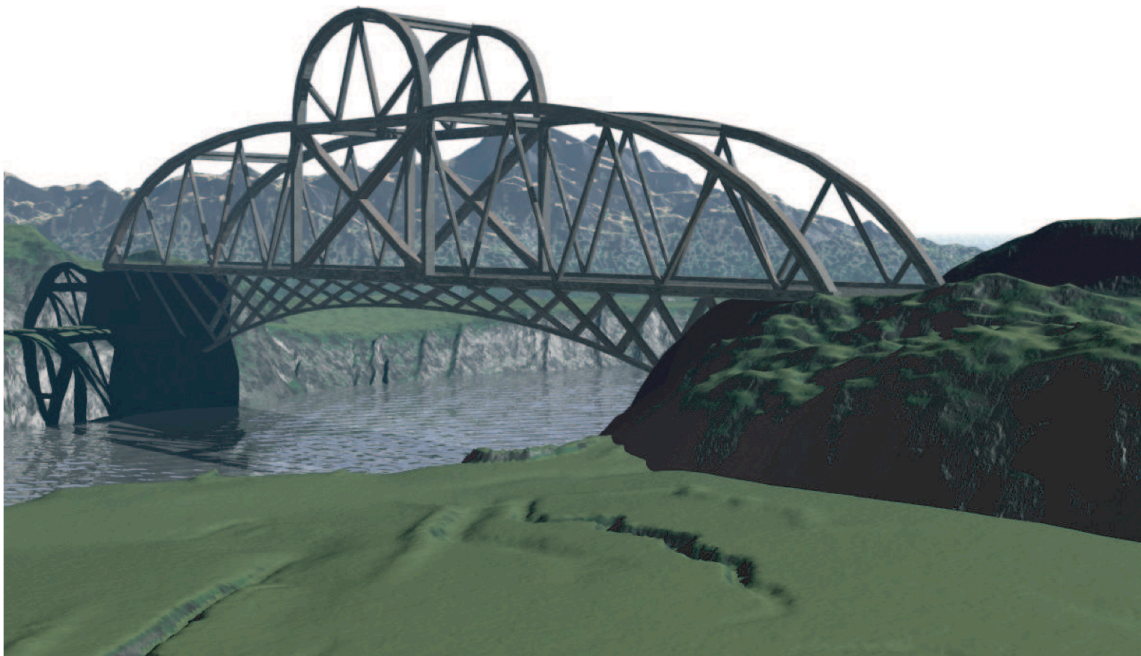


## Laboratoire 2

*Modélisation et vérification du comportement de véhicules autonomes sur un pont à voie unique\**

Cours : LOG670 – Langages formels et semi-formels  
Session : Hiver 2015  
Professeur(e) : Sylvie Ratté  
Modalité : Équipe  
Pondération : 15%

---



---

\* Laboratoire original du cours de « Modélisation formelle et systèmes répartis » de l'université Pierre et Marie Curie (2006, F. Kerdon)

## Introduction

Le projet présenté ci-après vise à vous initier à la modélisation et la vérification de systèmes répartis grâce aux automates temporisés et la logique CTL. À la fin de ce laboratoire, vous serez en mesure :

- D'utiliser un outil de modélisation d'automates temporisés;
- De modéliser des systèmes répartis simples;
- D'en faire la vérification avec des formules CTL;
- De tirer les conclusions découlant de ces analyses;
- De mieux saisir les problèmes entourant la modélisation et la vérification de systèmes de ce type.

Le projet se compose de deux parties : la modélisation de véhicules autonomes sur un pont à voie unique et la modélisation de véhicules prioritaires. Pour chaque partie, vous devez répondre à un ensemble de questions.

## 1 Modélisation de véhicules autonomes sur un pont à voie unique

Le système que nous considérons est composé des entités suivantes :

- VAA, qui représente un véhicule automatisé de type  $A$  (qui circule dans un sens donné sur le pont),
- VAB, qui représente un véhicule automatisé de type  $B$  (qui circule dans un sens donné sur le pont),
- CTRLP, qui représente le système de contrôle qui autorisera les VAA et les VAB à entrer sur le pont,
- P, qui représente les propriétés intrinsèques du pont.

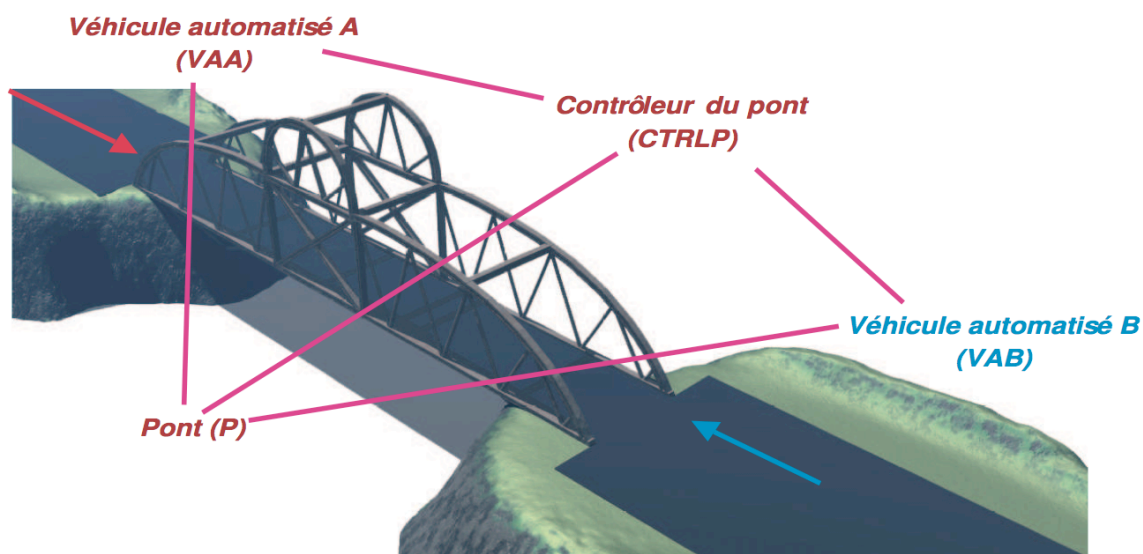
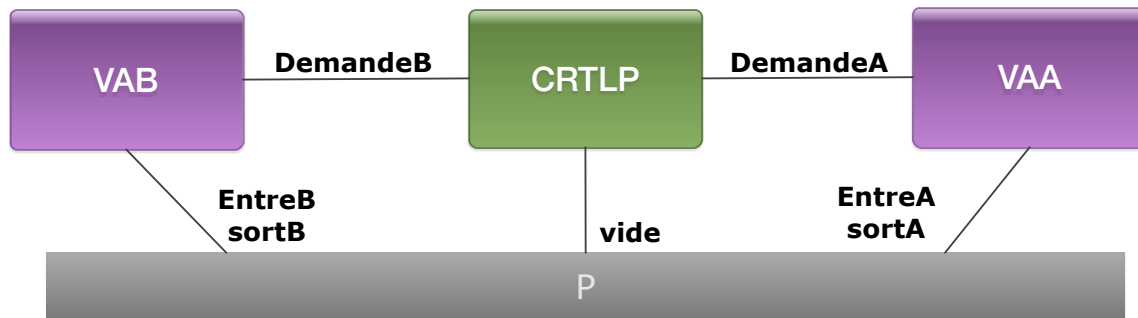


Figure 1. Relations entre les entités du système

Ces entités sont reliées suivant le schéma de la Figure 1. Chaque véhicule doit, avant d'entrer sur le pont, communiquer<sup>1</sup> avec le contrôleur associé pour en obtenir l'autorisation. Lorsqu'il obtient cette autorisation, il redémarre pour franchir le pont ; dans le cas contraire, il se met en attente. Le contrôleur doit quant-à-lui assurer que l'ouverture du pont à une catégorie de véhicule s'effectue de manière équitable, c'est-à-dire soit lorsque  $N_{alt}$  véhicules d'un même type sont passés sur le pont, soit à l'expiration d'une temporisation. On considérera que le système contient  $N_{VAA}$  VAA et  $N_{VAB}$  VAB. Enfin, la capacité du pont est de  $Capa_p$  véhicules, quelque soit leur type.



**Figure 2.** Architecture proposée pour le système.

On propose pour le système l'architecture indiquée en Figure 2. Cette figure spécifie des «services» que l'on attend du système mais sans en détailler la sémantique et les paramètres.

## Question sur la première partie

### Question 1.1 : modélisation des composants VAA et VAB

Modélisez le comportement d'un VAA et celui d'un VAB. Vérifiez que cette modélisation est correcte « localement ».

### Question 1.2 : modélisation du composant P

Modélisez le comportement des caractéristiques du pont assurées par le composant P. Vérifiez que cette modélisation est correcte « localement ».

### Question 1.3 : modélisation du composant CTRLP

Modélisez le comportement des caractéristiques du CTRLP. Vérifiez que cette modélisation est correcte « localement ».

### Question 1.4 : assemblage

Procédez à l'assemblage des composants que vous avez modélisé. Présentez, si cela est nécessaire, les composants supplémentaires que vous avez dû ajouter. Vérifiez que cet assemblage est cohérent et que les « propriétés triviales attendues » sont bien présentes dans cette spécification.

### Question 1.5 : vérification

Procédez à la vérification formelle du modèle pour les propriétés suivantes :

<sup>1</sup> On suppose l'existence d'un réseau fiable aux alentours du pont.

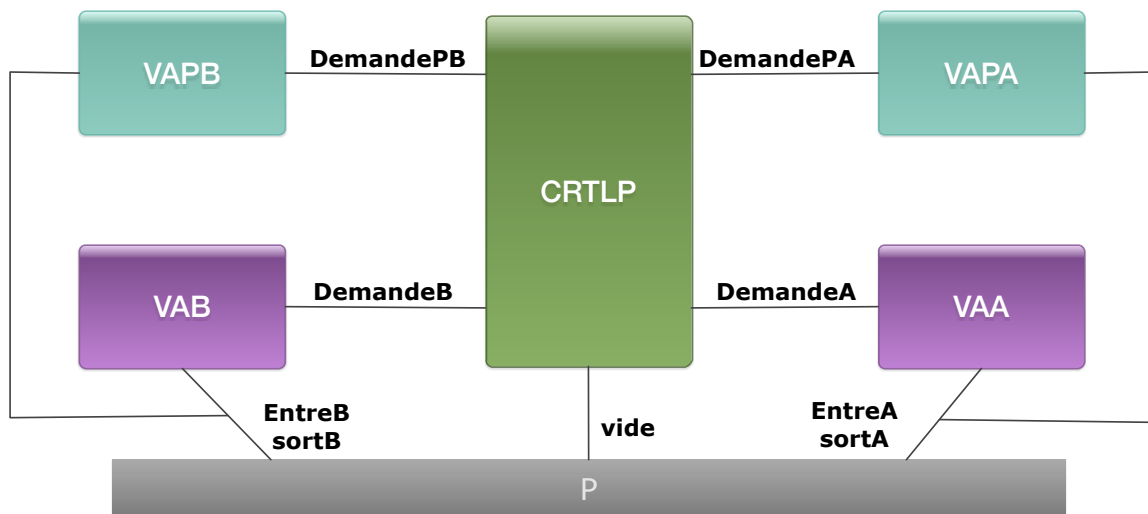
- $P_1$  : Il n'y a pas de collision (i.e. deux véhicules circulant en sens inverse) sur le pont.
- $P_2$  : Un véhicule qui arrive est certain de passer sur le pont à l'issue d'une durée bornée.

Vous exprimerez ces propriétés en des termes vérifiables (CTL) et utiliserez l'outil offert par UPPAAL pour démontrer leur validité.

## 2 Extension du système pour gérer des véhicules prioritaires

On considère désormais que le système possède deux nouveaux types d'entités :

- VAPA, qui représente un véhicule automatisé *prioritaire* de type  $A$  ; il a les mêmes caractéristiques qu'un VAA mais il doit entrer prioritairement sur le pont (c'est-à-dire avant qu'un véhicule non prioritaire VAB ou VAA n'entre sur le pont).
- VAPB, qui représente un véhicule automatisé *prioritaire* de type  $B$  ; il a les mêmes caractéristiques qu'un VAB mais il doit entrer prioritairement sur le pont (c'est-à-dire avant qu'un véhicule non prioritaire VAB ou VAA n'entre sur le pont).



**Figure 3.** Architecture proposée pour le système.

On propose pour cette extension du système l'architecture indiquée en Figure 3. Comme précédemment, cette figure spécifie des « services » que l'on attend du système mais sans en détailler la sémantique et les paramètres.

### Question sur la deuxième partie

#### Question 2.1 : modélisation des composants VAA et VAB

Modélisez le comportement d'un VAA et celui d'un VAB. Vérifiez que cette modélisation est correcte « localement ».

### **Question 2.2 : modélisation des composants VAPB et VAPB**

Modélisez le comportement d'un VAPA et celui d'un VAPB. Vérifiez que cette modélisation est correcte « localement ».

### **Question 2.3 : modélisation du composant P**

Mettez à jour si besoin est le comportement des caractéristiques du pont assurées par le composant P. Vérifiez que cette modélisation est correcte « localement ».

### **Question 2.4 : modélisation du composant CTRLP**

Mettez à jour si besoin est le comportement des caractéristiques du CTRLP. Vérifiez que cette modélisation est correcte « localement ».

### **Question 2.5 : assemblage**

Procédez à l'assemblage des composants que vous avez modélisé. Vérifiez que cet assemblage est cohérent et que les « propriétés triviales attendues » sont bien présentes dans cette spécification.

### **Question 2.6 : vérification**

Procédez à la vérification formelle du modèle pour les propriétés suivantes :

- $P_1$  : Il n'y a pas de collision (i.e. deux véhicules circulants en sens inverse) sur le pont.
- $P_2$  : Un véhicule normal qui arrive est certain de passer sur le pont à l'issue d'une durée bornée.
- $P_3$  : Un véhicule prioritaire qui arrive est certain de passer sur le pont à l'issue d'une durée bornée avant tout autre véhicule normal qui n'est pas encore entré sur le pont.

Vous exprimerez ces propriétés en des termes vérifiables (CTL) et utiliserez l'outil offert par UPPAAL pour démontrer leur véracité.

## **Remise**

Chaque équipe doit remettre :

Un lien qui nous permettra d'accéder aux descriptions, vérifications et fichiers nécessaires (dans l'ordre spécifié dans la structure du rapport).