Université de Namur

2023– 2024

Vérification de Modèles
INFOM471

Sujet de Labo

1 Introduction

Ce document décrit le travail de Labo demandé dans le cadre du cours Validation de Modèles (InfoM471). Le but est double : spécifier un système critique à l'aide du paradigme synchrone, et vérifier son comportement à l'aide d'un prouveur Smt, à l'aide de l'outil Esterel Scade.

La thématique porte sur un contrôleur de portes de sortie d'un tramway : celui-ci permet d'actionner de manière sécurisée les portes ainsi que les passerelles rétractables facilitant le passage d'éléments roulants (fauteuils roulants pour handicapés, poussettes, etc.)

Organisation du Document. Le sujet est composé de quatre parties : en Section 2 est décrit le rôle du contrôleur de manière plus précise, en insistant sur l'interaction avec son environnement ; la Section **??** donne un guide d'implémentation du contrôleur tandis que la Section 4 indique les étapes nécessaires à la vérification de deux propriétés de sûreté importantes.

2 Description

Quatre éléments, constituant l'environnement du contrôleur, communiquent directement avec celui-ci au travers de signaux prédéfinis :

Porte (Door) Lorsque le tram est arrêté en station, le contrôleur doit ouvrir les portes (openDoor) pour laisser passer les passagers, puis les refermer (closeDoor) lorsque le tramway est sur le point de redémarrer. On suppose que les portes réagissent correctement aux signaux, c'est-à-dire qu'elles s'ouvrent et se ferment effectivement à l'arrivée des signaux ; par contre, on ne sait pas a priori combien de temps ces opérations prennent : l'état de la porte est connu grâce à un capteur renseignant sur son statut (DoorStatus), et le contrôleur doit maintenir le signal d'ouverture ou de fermeture tant que la porte n'a pas terminé son mouvement.

Passerelle (Bridge) En station, et en fonction de la demande des passagers, le contrôleur peut déployer une passerelle (deploy), et la rétracter (retract) lorsque le tramway s'apprête à démarrer. Le comportement de la passerelle est similaire à celui de la porte : un capteur renseigne sur le statut de la passerelle (BridgeStatus).

Usager (User) Un usager se contente d'actionner des boutons pour demander l'ouverture d'une porte (requireDoor) ou le déploiement d'une passerelle (requireBridge). Lorsque le déploiement de passerelle est demandé, cela implique implicitement d'ouvrir la porte (même sans action sur le bouton correspondant). Le contrôleur doit filtrer et enregistrer les demandes pour pouvoir les traiter en toute sécurité : en particulier, appuyer sur ces boutons pendant que le tramway roule ne provoque aucune action jusqu'à ce qu'une station soit atteinte ; un usager peut cependant demander l'ouverture de porte ou le déploiement de passerelle quand le tram est déjà arrêté.

Tramway (Tramway) Le tramway renseigne le contrôleur sur les conditions de roulage. Il envoie un signal inStation lorsqu'il s'arrête à une station, et un signal immDeparture (départ imminent) lorsque le chauffeur appuie sur un bouton pour signaler la fin du ramassage de passager afin de commander la fermeture des portes de la rame et ainsi pouvoir démarrer. Le contrôleur attend alors la commande secured, signalant que les portes sont effectivement fermées (et les passerelles rétractées) avant d'autoriser le démarrage.

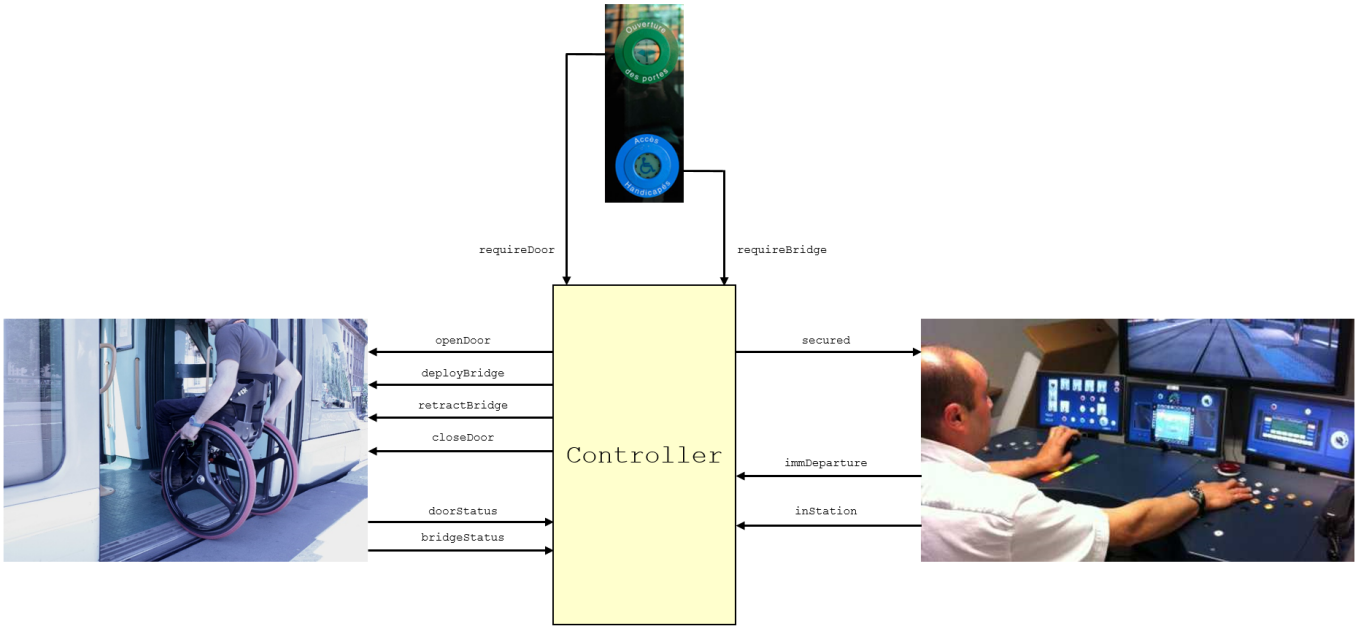

FIGURE 1 – Schéma de Principe du Contrôleur du Tramway. Le contrôleur reçoit le statut de la rame : si elle est parquée en station (inStation, et si elle doit repartir (immdeparture) et lui envoie l'autorisation de départ (secured, lorsque la passerelle est effectivement rétractée et la porte fermée). Le contrôleur actionne la porte et/ou la passerelle (openDoor et deployBridge) en tenant compte de la volonté de descendre des usagers (requireBridge et requireDoor).

Le contrôleur joue donc deux rôles essentiels :

- il garantit le bon fonctionnement du tramway, en interdisant celui-ci de rouler avec les portes ouvertes ou les passerelles déployées, et en s'assurant que les passerelles soient toujours déployées avant que le porte ne soit ouverte ;
- il satisfait les demandes des usagers en retardant les demandes d'ouverture ou de déploiement faites pendant le roulage à l'arrêt dans la prochaine station, et en ignorant ces demandes lorsque il y a départ immédiat.

Afin de valider l'implémentation du contrôleur, nous vérifierons deux propriétés de sûreté importantes :

- le tramway ne peut pas rouler avec la porte ouverte ou la passerelle déployée ;
- la passerelle ne peut pas bouger (être déployée ou rétractée) lorsque la porte est ouverte.

Idéalement, il faudrait aussi vérifier une propriété de vivacité primordiale : toute demande d'ouverture de porte (ou de déploiement de passerelle) est finalement honorée. En effet, il serait toujours possible d'adopter un comportement "dégénéré" pour garantir les propriétés de sûreté précédentes : ne jamais ouvrir la porte !

3 Implémentation

La Figure 1 donne un schéma de principe des différents composants entrant en action dans la modélisation du fonctionnement de la porte, en explicitant les commandes échangées.

La première étape consiste à spécifier le comportement des composants annexes : que se passe-t-il lorsqu'un usager appuie sur le bouton ? Comment se comportent la porte et la passerelle ?

▻ **Question 1** ◅
Spécifier un opérateur Button correspondant à l'effet d'un bouton : lorsque quelqu'un appuie sur le bouton (faisant ainsi changer une fois la valeur du flux de données), le bouton reste éclairé, simulant ainsi la demande d'ouverture de porte ou de déploiement de passerelle.

▻ **Question 2** ◅
Spécifier le comportement de la porte par une machine à états qui renseigne en sortie son statut (doorStatus) : la porte est soit ouverte / fermée ; soit en cours d'ouverture / fermeture.

▷ **Question 3** ◁
Spécifier le comportement de la passerelle de la même façon.

▷ **Question 4** ◁
Que doit rajouter le contrôleur pour assurer la synchronisation du déploiement de la passerelle et de l'ouverture de la porte ?

La seconde étape consiste à relier les éléments entre eux au travers du contrôleur : quand le contrôleur décide-t-il d'actionner l'ouverture ou la fermeture de porte (respectivement, le déploiement ou la rétraction de passerelle) ?

▷ **Question 5** ◁
Spécifier l'envoi de la commande d'ouverture de porte / déploiement de passerelle, lorsque la rame se trouve en station et que la porte ou la passerelle a été demandée. Ne pas oublier que la commande doit être maintenue jusqu'à l'ouverture ou le déploiement effectif.

▷ **Question 6** ◁
Spécifier l'envoi de la commande de fermeture de porte / rétraction de passerelle, lorsque le départ est immédiat et que la porte est ouverte (ou en cours d'ouverture) ou que la passerelle est déployée (ou en cours de déploiement).

▷ **Question 7** ◁
Spécifier l'autorisation de départ émanant du contrôleur. Trois cas sont possibles.
— La porte est déjà fermée (et la passerelle rétractée) : le tramway peut redémarrer ;
— La porte est ouverte (ou en cours d'ouverture) : il faut attendre qu'elle soit fermée pour redémarrer ;
— La passerelle est déployée (ou en cours de déploiement) : il faut attendre qu'elle soit rétractée, et que la porte se referme.

4 Vérification

Les deux propriétés que nous cherchons à vérifier traduisent le fonctionnement sécurisé du tramway, dont le comportement est spécifié par le contrôleur :

SecuredDriving le tramway ne peut jamais rouler avec la porte ouverte ou la passerelle déployée ;

SafeBridge la passerelle ne peut pas s'activer (c'est-à-dire se déployer ou se rétracter) lorsque la porte est ouverte.

Ces deux propriétés s'expriment simplement avec les opérateurs temporels disponibles dans la librairie Scade.

▷ **Question 1** ◁
Spécifier les opérateurs SecuredDriving et SafeBridge exprimant les deux propriétés de sûreté, à l'aide d'opérateurs observateurs.

Malheureusement, ces propriétés ne sont pas vraies dans l'absolu : elles dépendent de l'environnement dans lequel est défini le contrôleur. Afin de valider ces hypothèses, il faut définir des assertions sur l'environnement dans lequel est utilisé le contrôleur, et s'assurer que ces assertions sont vérifiées à chaque utilisation (instanciation) de l'opérateur correspondant.

▷ **Question 2** ◁
Spécifier des assertions sur le bon fonctionnement de la porte et de la passerelle, indiquant que :
— La porte (respectivement, la passerelle) est initialement fermée (respectivement, rétractée) ;
— Si openDoor (respectivement, deployBridge) devient vrai, alors la porte s'ouvrira (resp., la passerelle se déploiera) plus tard ;
— De même, si closeDoor (resp. retractBridge) devient vrai, alors la porte se fermera (resp. la passerelle se rétractera) plus tard.
— openDoor et closeDoor (resp. deployBridge et retractBridge) ne peuvent pas être vrais en même temps.

▷ **Question 3** ◁
Le tramway a un comportement moins contraint : il peut entrer en station n'importe quand (on ne suppose rien sur le nombre de stations ou leur espacement), mais ne peut en repartir qu'après réception

du signal immDeparture par le conducteur et quand la porte et la passerelle sont sécurisées (secured). Spécifier des assertions indiquant que :

— Il y a au moins une occurrence de immDeparture entre les évènements d'arrivée et de départ de station ;

— Il y a au moins une occurrence de secured entre ces mêmes évènements.

▻ **Question 4** ◅

Afin de vérifier le comportement, il reste à :

— Assembler les différents éléments pour réaliser la vérification ;

— Documenter les éventuelles modifications aux opérateurs suivant les erreurs trouvées par Design Verifier.