Project Formele Systeemmodellering voor Software

Bruno Corijn, Jasper Van der Jeugt, Toon Willems

13 januari 2013

1 Deel 2: TLA/TLC

Het oorspronkelijk protocol is terug te vinden in de Trein.* files, die we eerst zullen bespreken. Vervolgens kijken we naar wat er verbeterd moet worden , deze veranderingen zijn terug te vinden in de BeterTrein.* bestanden.

1.1 Originele specificatie en vereisten

In de eerste versie zijn enkel het protocol en de vereisten gespecifiëerd in de opgave geïmplementeerd. Hiervoor gebruiken we de volgende variabelen:

- `deuren` geeft aan op de conducteur de passagiersdeuren heeft gesloten.
- `conductdeurDeur` geeft aan of de conducteur zijn eigen deur heeft gesloten.
- `ac` geeft aan of het Action Completed signaal is gegeven.
- `seinlicht` bevat de huidige kleur van het seinlicht. Dit kan rood of wit zijn.
- `vertrek` geeft aan of de trein vertrokken is.

In de initiële toestand zijn al deze variabelen 0, buiten het seinlicht dat op rood zal staan. Deze veriabelen zullen van waarde veranderen aan de hand van de volgende acties:

- `Fluitsignaal` Vereist dat de deuren open zijn en het seinlicht op rood staat. Hierdoor worden de deuren gesloten.
- `Action` Als de deuren dicht zijn, kan het AC signaal gegeven worden.
- `Seinlicht` Als het AC signaal gegeven is, kan het seinlicht van kleur veranderen naar wit.
- `Vertrek` Indien het seinlicht op wit staat kan de trein vertrekken.
- `Reset` Zet na vertrek van de trein alle variabelen terug naar hun oorspronkelijke staat.
- `Deur` Als de trein vertrokken is kan de conducteur zijn deur sluiten.

Daarnaast hebben we ook nog specificaties `Next` dat altijd een van de bovenstaande acties zal zijn, `Live` die ervoor zorgt dat de variabelen correct blijven en `Spec` die specifiëert dat het programma altijd start uit de initiële toestand, via `Next` in de huidige toestand kan belanden en dat `Live` altijd geldt.

Als laatste hebben we de veiligheid- en fairnessvereisten van dit systeem die geïmpliceerd worden door `Spec`. Dit zijn de volgende:

- `VertrekNaAc` Na het geven van het AC signaal zal het seinlicht verspringen van kleur.
- `RoodSeinlichtDefault` In de begintoestand is het seinlicht altijd rood.
- `Fairness` Als het seinlicht wit is, zal de trein vertrekken.
- `Veiligheid` De trein mag niet vertrekken zonder de conducteur.
- `OoitVertrek` De trein al ooit vertrekken.

1.2 Problemen

Door de automatische modelchecker zien we dat de veiligheidsvereiste kan geschonden worden door het bestaande protocol, dit zullen we oplossen in de verbeterde versie.

1.3 Verbeteringen

Om te voorkomen dat de trein kan vertrekken zonder de conducteur is er een extra regel toegevoegd aan de `Vertrek` actie, die vereist dat de deur van de conducteur gesloten is alvorens de trein kan vertrekken. Hierdoor is er wel voldaan aan de veiligheidsvereiste

1.4 Verificatie

De output en configuratie van de automatische verificatie van beide versies zijn te vinden als bijlages aan ons verslag.