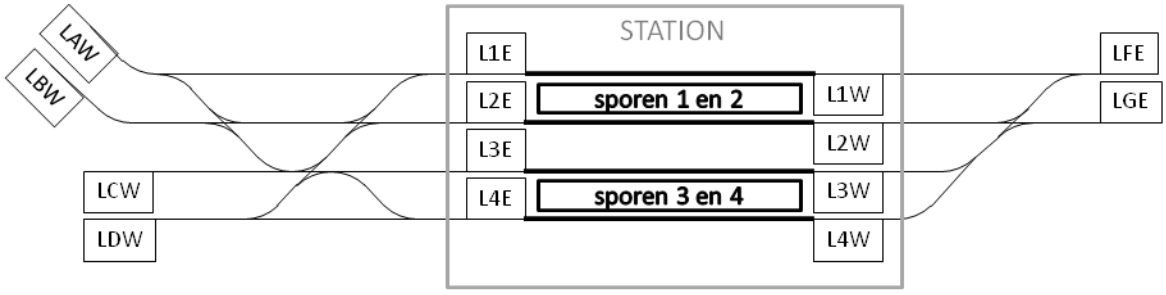
Project Formele Systeemmodellering voor Software: Specificatie en verificatie in TLA+/TLC

Eric Laermans (eric.laermans@UGent.be)

2018-03-30

1 Inhoud

De bedoeling van het project is een TLA+-specificatie te schrijven voor een (vrij eenvoudig) spoorsysteem met wissels, en te verifiëren (met de model-checker TLC bijvoorbeeld) dat deze specificatie voldoet aan de gewenste (veiligheids)vereisten.



Figuur 1: Schema van sporen in een station

Fig. 1 toont het schema van de te modelleren spoorsectie. Er zijn 2 sporen in de "oostelijke" richting (rechts op de figuur): "F" en "G". En er zijn 4 sporen in de "westelijke" richting (links op de figuur): "A", "B", "C" en "D". Daartussen zijn de 4 perrons of sporen in het station zelf: genummerd van 1 tot en met 4.

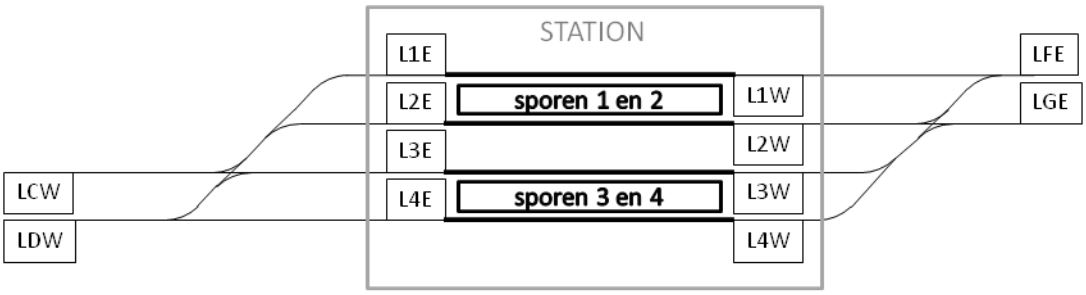
Er zijn 12 wissels op de verschillende sporen die toelaten om van spoor te veranderen. Alle wissels hebben twee mogelijke standen. Zo laat de meest westelijke wissel op het westelijke spoor A toe om ofwel op spoor A rechtdoor te blijven rijden (eerste stand), ofwel in oostelijke richting over te gaan van spoor A naar spoor B (tweede stand). De meest westelijke wissel op het westelijke spoor B is iets complexer. Deze wissel kan ofwel doorgaand verkeer op spoor B toelaten en verkeer dat van spoor A naar spoor C wisselt (in oostelijke richting) (eerste stand), ofwel verkeer toelaten dat van spoor A naar spoor B wisselt (in oostelijke richting) en verkeer dat van spoor B naar spoor C wisselt (tweede stand). Voor treinen die in westelijke richting rijden is de werking analoog.

Er zijn ook 14 lichtseinen die het verkeer controleren. De namen van deze lichtseinen zijn gegeven volgens het spoor en de richting van de trein. Zo betekent L1E het lichtsein voor een trein op spoor 1, komende uit oostelijke ("Eastern") richting. En LBW staat voor het lichtsein voor een trein op spoor B, komende uit westelijke ("Western") richting. Deze lichtseinen hebben drie mogelijke standen:

- Groen: de trein mag doorrijden en het eerstvolgende signaal dat hij tegenkomt is groen of geel
- Geel: de trein mag doorrijden en het eerstvolgende signaal dat hij tegenkomt is rood
- Rood: de trein moet stoppen

Eens een trein voorbij een groen sein gereden is, verspringt dit sein op rood. De treinen moeten de signalen altijd respecteren.

Mocht u te veel problemen ondervinden bij de modellering/verificatie van het volledige model (te lange rekentijden voor de verificatie bij voorbeeld, dan kan u in eerste instantie een eenvoudigere versie trachten te modelleren met een verminderd aantal (westelijke) sporen, zie Fig. 2.



Figuur 2: Schema van sporen in een station (eenvoudigere versie)

Wat verwachten we van dit systeem?

De eerste categorie vereisten zijn natuurlijk de *veiligheidsvereisten*. Er mogen nooit twee treinen tegelijk op hetzelfde spoor rijden of elkaars weg kruisen (wat neerkomt op het tegelijk gebruiken van dezelfde wissel). Zo zal in Fig. 1 een trein die van spoor A naar spoor 4 rijdt, tijdelijk sporen A, B, C en D blokkeren voor ander treinverkeer. Een trein die in Fig. 1 van spoor B naar spoor 1 rijdt, blokkeert tijdelijk sporen A en B, maar blokkeert ook verkeer van sporen C en D naar spoor 2 (de trajecten gebruiken dezelfde wissel). De treinen moeten ook de lichtseinen respecteren en de lichtseinen mogen geen aanleiding geven tot gevaarlijke situaties.

De tweede vereiste is een *fairnessvereiste*, namelijk dat een trein niet eindeloos opgehouden wordt door een rood lichtsein.

Wat verwacht ik van u?

- een formele specificatie (TLA+) van dit systeem
- een formele vertaling van de veiligheids- en fairnessvereisten voor dit systeem
- de verificatie dat uw specificatie voldoet aan de veiligheids- en fairnessvereisten (gebruik van de model-checker TLC is aangewezen)

2 Groepen

Zoals gezegd, wordt dit project in groepen van 4 (of 3) personen uitgevoerd. De eerste opdracht is dus onderling af te spreken om deze groepen samen te stellen. Laat mij liefst zo snel mogelijk de samenstelling van de verschillende groepen weten (via de "Groepen"-functionaliteit van Minerva). Aarzel ook niet om het forum op Minerva te gebruiken om een oproep te lanceren om een groep te vormen.

Ik verwacht slechts één verslag per groep.

Wie praktische moeilijkheden zou ervaren om bij een groep aan te sluiten (bv. werkstudent), neemt best (voldoende snel) contact met mij op.

3 Rapportering

Tussentijdse rapportering

Ik verwacht van elke groep een *korte* tussentijdse e-mail-rapportering (deadlines zijn 27 april en 11 mei, telkens op vrijdag, om 22u00). Hierin vermeldt u kort (langer dan een halve bladzijde is zeker niet nodig) wat de bijdrage van elk lid van de groep geweest in de vorige periode (taak + geschatte tijdsduur) en wat u in de periode tot aan het volgende rapport voor dit project plant. Wees hier eerlijk in. Het is inderdaad mogelijk dat tijdens een van deze perioden de activiteit gering is of dat u niet altijd uw gewenste doelstellingen haalt.

U zal niet afgerekend worden op deze tussentijdse rapportering. Het doel is voor mij om een overzicht te hebben over de vooruitgang van het project bij iedereen en tijdig op de hoogte te zijn van het niet-functioneren van een van de groepsleden.

Finale rapportering

Het finale resultaat van het project (waarop u beoordeeld wordt) bestaat uit:

- de formele specificatie van het systeem (in TLA+)
- een formele vertaling van de veiligheids- en fairnessvereisten voor dit systeem
- de formele verificatie met behulp van de model checker (TLC)
- het rapport zelf

In het rapport verwacht ik de volgende elementen:

- een duidelijke uitleg van de specificaties (zowel de specificaties van de werking van het protocol als de specificaties van de veiligheids- en fairnessvereisten); ik zou de TLA+-code eigenlijk niet moeten lezen en toch moeten kunnen begrijpen wat er gespecificeerd en geverifieerd is
- een vermelding van en uitleg voor de eventuele vereenvoudigingen die u gemaakt heeft (deze kunnen soms nodig zijn om de specificatie met de model checker verifieerbaar te houden)
- een conclusie over de bekomen resultaten

Bij voorkeur dient u het project in via de dropbox van Minerva als een archiefbestand met daarin:

- het verslag
- de TLA+-specificaties (.tla-bestanden)
- de TLC-configuratiebestanden (.cfg-bestanden)
- de verificatie-output van TLC

Vergeet hierbij niet de naam van uw groep te vermelden.

U mag ook afkortingen aanbrengen op het schema, dat meegegeven is als powerpoint-bestand op minerva, zodat u het in zijn oorspronkelijke gedaante kan gebruiken.

4 Evaluatie

De evaluatiecriteria zijn:

- de volledigheid en correctheid van de specificaties en vereisten (50%)
- de volledigheid en correctheid van de verificatie (25%)
- de kwaliteit van het verslag (25%)
- de tijdigheid van de rapportering

De **uiterste** indiendatum voor de finale rapportering van dit project is **25 mei 2018 (22u00)**.