Verslag Tinlab Advanced Algorithms

R. Karajev, M. Steijger
0851997 0938713

15 april 2021

Inhoudsopgave

1 Inleiding

Voor Tinlab Advanced Algorithms wordt het methode Model Checking gegeven [2]. Dit onderwerp wordt getoetst door middel van een eindopdracht. Het doel van deze opdracht is een model aan te leveren van een compleet geautomatiseerd sluis. Daarbij is het de bedoeling dat op basis van opgestelde requirements bepaalde eigenschappen binnen dit model geverifieerd worden. Dit verslag word geschreven om de keuzes die tijdens het process zijn gemaakt te onderbouwing en vast te leggen. Hierin is ook te lezen alles over de model en de werking ervan. Tot slot wordt aan het eind van dit verslag geverifieerde eigenschappen gepresenteerd.

2 Requirements

Voor deze opdracht is gekozen om een model te maken van een schutsluis. Als begin is het handboek voor het ontwerpen van schutsluizen bekeken. [4]. Gezien de wens van de opdrachtgever voor het aanleveren van een model van een geautomatiseerde sluis is er voor gekozen om de volgende functionele eis dat in het handboek gevonden is als uitgangspunt te nemen voor het opstellen van de requirements voor deze opdracht.

"De functionele eisen van een schutsluis zijn primair bedoeld voor de scheepvaart. Als belangrijkste algemene functionele eis geldt dat de scheepvaart zodanig **snel** *en* **veilig** *de sluis moet kunnen passeren."*

Voor deze opdracht wordt dus ook een schutsluis gemodelleerd die zo velig mogelijk functioneert zonder dat deze de scheepvaart belemert. Om dit te kunnen doen is hierbij als eerst gekeken naar een document waarbij algemeen opbouw van Julianasluis 2 beschreven wordt om een opbouw van een schutsluis beter te begrijpen [1]. Op basis van deze opbouw is er voor gekozen om een simplistische model ervan te bouwen. Een simplistische model wordt gebruikt om ervoor te zorgen dat bij het modeleren de focus vooral ligt op de kernfunctionaliteiten. Zo kunnen de veiligeisen die betrekking hebben tot de functionaliteit dan ook geverifieerd worden.

Voordat een model opgesteld wordt, wordt er als eerst naar een functionele omschrijving sluitprocess gekeken te vinden in artikel [3]. Daaruit is informatie verkregen over functionering van een sluisprocess. In dit document zijn ook aanvullende functionele eisen gevonden wat betreft het veiligheid. Deze eisen worden gebruikt als basis om te indentificeren welke risico's er tijdens een sluitprocess bestaan. Tot slot wordt met behulp van deze informatie eigen veiligheideisen geformuleerd.

2.1 Veiligheidseisen

Sluisdeuren

1. Ten alle tijden mag er maar één sluisdeur open zijn.
   (*De reden hiervoor is zodat het waterhoogteverschil altijd behouden wordt.*)

2. Een sluisdeur mag alleen open als de waterniveau aan beiden kanten van de sluisdeur gelijk is.
   (*Dit is een belangrijke veiligheideis om ongecontroleerde water verplaatsing te voorkomen, waarbij mogelijk letsel zou kunnen onstaan.*)

3. Ten alle tijden mag een deur alleen aangedreven worden als het invaarsein het sein 'verboden voor doorvaart' of 'sperren' aangeeft.

4. Tijdens het nivelleren dienen ten alle tijden de sluisdeuren gesloten te zijn en scheepvaartseinen het sein 'verboden voor doorvaart' aangeven.
   (Dit is nodig om ongeschaad een schip van een waterhoogteniveau naar een ander waterhoogteniveau te brengen.)

Ricketschuiven

1. Ten alle tijden mag een ricketschuif alleen open als de ricketschuif in de tegenovergestelde sluisdeur gesloten is.
   (*Dit voorkomt de situatie waarbij er verbinding is tussen hoogland en laagland water.*)

2. Ten alle tijden mag een ricketschuif alleen open als de tegenovergestelde sluisdeur gesloten is.
   (*Dit zorgt ervoor dat waterhoogteniveau veilig aangepast kan worden.*)

Scheepvaartseinen

1. Ten alle tijden mag er maar aan één kant een scheepvaartsein het sein 'vrij voor doorvaart' aangeven.
   (*Dit voorkomt miscommunicatie en zorgt voor snel en veilige scheepvaart verkeer.*)

2. Ten alle tijden mag het scheepvaartsein 'vrij voor doorvaart' alleen worden afgegeven als de betrokken sluisdeur volledig geopent is.
   (*Dit zorgt ervoor dat schepen veilig het sluis binnen kunnen varen of verlaten zonder mogelijke ongelukken.*)

Noodstop

1. Ten alle tijden kan een noodstop worden ingeschakkeld.
   (*Noodstop zorgt ervoor dat alle componenten per direct gestopt/uitgezet worden.*)

2. Na het indrukken van de noodstop moet deze ook weer gereset kunnen worden.

3. Sluisdeuren moet ten alle tijden tot een noodstop kunnen worden gebracht.

4. Na het resetten van de noodstop dienen de sluisdeuren te hervatten met de onderbroken process.
   (*Er is afweging gemaakt voor een simplistisch model, daarom wordt deze requirement dan ook niet geimplementeerd en dus ook niet geverifieerd.*)

5. Ricketschuiven moeten ten alle tijden tot een noodstop kunnen worden gebracht waarbij de ricketschuiven per direct dienen te sluiten.

6. Na het resetten van de noodstop dienen de ricketschuiven naar hun originele positie te worden gebracht.

7. Scheepvaartseinen kunnen ten alle tijden tot een noodstop worden gebracht waarbij het sein 'buiten gebruik' aangegeven wordt.

3 Specificaties

Voor deze opdracht worden twee sluishoofden gemodelleerd zodat deze samen een schutsluis vormen. Zo kan dan ook vooral de focus liggen bij veilig functioneren. Per sluishoofd zijn de volgende keuzes gemaakt:

- *Sluisdeur*
  - Voor de sluisdeur is er gekozen om model te maken van puntdeuren. Dit zijn twee deuren die gebruikt kunnen worden voor scheiding tussen de kolk en de buitenwater. Om dit model simpel te maken wordt hierbij één deur gemodelleerd die het twee delige puntdeuren representeert. (*Gezien identieke functionaliteit heeft het geen zin om twee keer deze deur te gaan modeleren.*)
  - Een sluisdeur bestaat uit 4 toestanden en 1 noodtoestand. De toestanden zijn 'openen', 'open', 'sluiten', 'gesloten' en als laatste is er ook nog een 'noodtoestand'.
  - Openen en sluiten van de sluisdeur wordt door middel van een timer bijgehouden. Het sluiten of openen van de sluisdeur duurt 1 minuut.
  - Om aan *Noodstop* requirement 4 te voldoen wordt het openen of sluiten van de sluisdeur bijgehouden door middel van een status variabele.
- *Ricketschuif*
  - Voor de nivelleermiddel is er keuze gemaakt om een ricketschuif ervoor te modeleren. Een ricketschuif is een opening in een sluisdeur dat de waterpeil in de kolk kan controleren.
  - Een ricketschuif bestaat uit 4 toestanden. De toestanden zijn 'openen', 'open', 'sluiten' en 'gesloten'. Gezien *Noodstop* requirement 5 en 6 worden 2 extra tussen toestanden gebruikt om de ricketschuif naar de betreffende toestand te kunnen brengen.
  - Openen en sluiten van de ricketschuif wordt door middel van een timer bijgehouden. Het sluiten of openen van de ricketschuif duurt minder dan 1 minuut.
  - Om aan *Noodstop* requirement 5 en 6 te voldoen wordt het openen of sluiten van de ricketschuif bijgehouden door middel van een status variabele.
- *Scheepvaartsein*
  - Voor de scheepvaartsein is gekozen om per sluisdeur twee scheepvaartseinen te modeleren. Één voor buiten de sluis en één voor binnen de sluis. Hierbij wordt één model voor twee verschillende scheepvaartseinen gebruikt met een variabele verschill in de 'noodtoestand' waar voor de binneste geld sein is 'uit' en de buiteste het sein is 'buiten gebruik'.

  - De scheepvaartsein bestaat uit 3 toestanden en een 1 noodtoestand. Deze zijn als volgt gedefineerd:
    * 'buiten gebruik'/'noodtoestand' = Rood Rood / Uit
    * 'verboden voor doorvaart' = Rood
    * 'gereed maken voor doorvaart' = Rood Groen
    * 'vrij voor doorvaart' = Groen

- *Noodstop*
  - Voor de noodstop is gekozen om een model te maken van een drukknop die na het drukken weer gereset moet worden naar zijn originele positie.
  - Op het moment dat de noodstop is ingedrukt, moeten alle onderdelen per direct in voor hun betreffende noodtoestand gaan.

- *Simulatie*
  - Om een schutsluis te kunnen simuleren worden de besproken onderdelen gemaakt. Deze onderdelen worden gecombineerd met een simulatie voor scheepvaart om uiteindelijk tot een werkende model te komen die de werking van de schutsluis simplistisch uitbeeld. Dit wordt gedaan in de hoofdmodel waar alle logica van de schutsluis uitgewerkt wordt.
  - Per kant worden 2 schepen geschut. Aantal schepen per kant wordt bijgehouden door middel van een getal. Elke keer dat een schip geschut is wordt deze getal verminderd met 1.
  - Bij het begin toestand geldt voor alle onderdelen dat deze in toestand 'gesloten' bevinden. Voor scheepvaartseinen, deze dienen in de toestand 'verboden voor doorvaart' zich te bevinden. Bij het schutten van de schepen wordt de volgende process doorlopen:

    * Scheepvaartsein (laagland) in toestand 'gereed maken voor doorvaart'
    * Sluisdeur (laagland) openen
    * Scheepvaartsein (laagland) in toestand 'vrij voor doorvaart'
    * Sluisdeur (laagland) sluiten
    * Scheepvaartsein (laagland) in toestand 'verboden voor doorvaart'
    * Ricketschuif (hoogland) openen
    * Nivelleren: hoogland – laagland
    * Ricketschuif (hoogland) sluiten
    * Scheepvaartsein (hoogland) in toestand 'gereed maken voor doorvaart'
    * Sluisdeur (hoogland) openen
    * Scheepvaartsein (hoogland) in toestand 'vrij voor doorvaart'
    * Sluisdeur (hoogland) sluiten

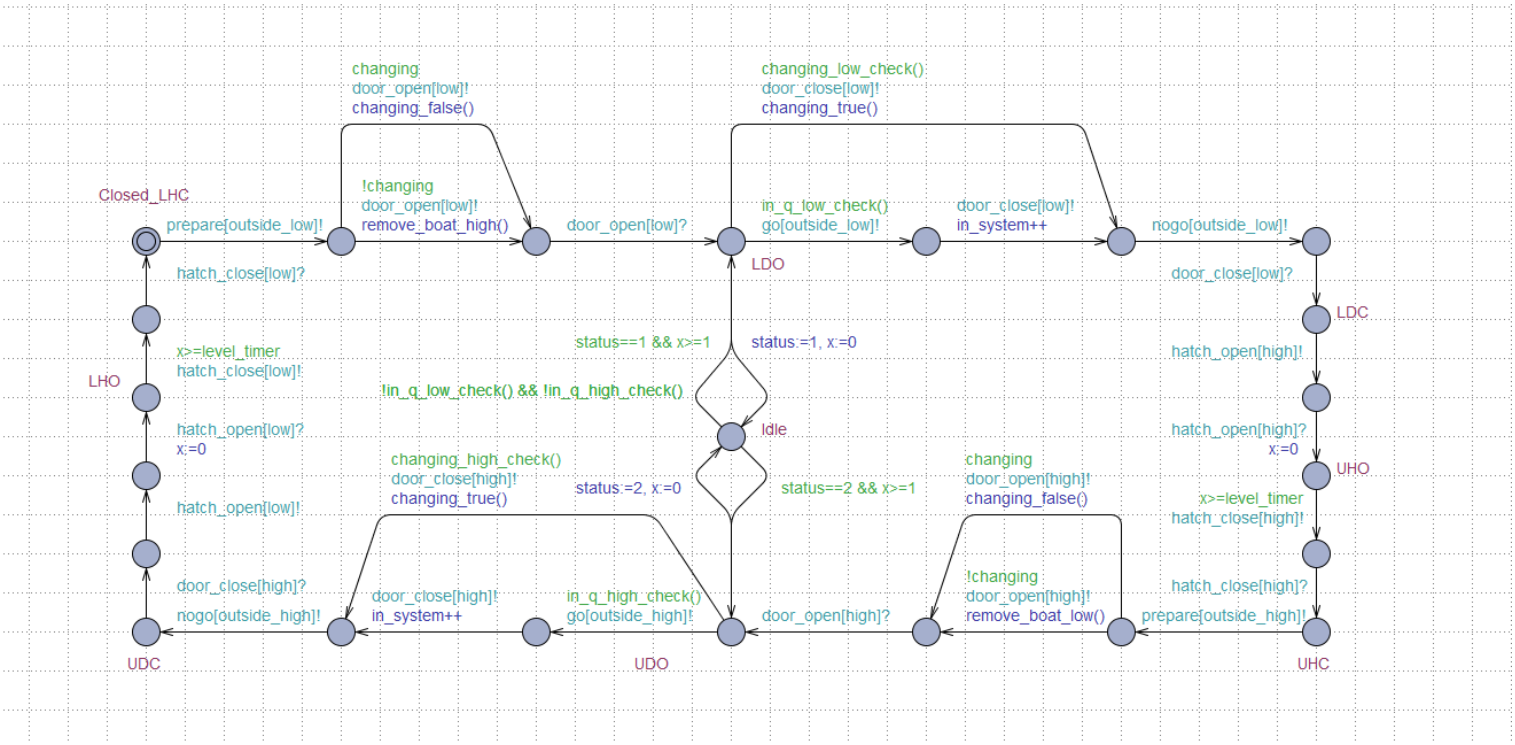
* Ricketschuif (laagland) openen
* Nivelleren: laagland – hoogland
* Ricketschuif (laagland) sluiten

4 Gemodelleerde onderdelen

De schutsluis model wordt een simplistische model van Julianasluis 2. Deze model wordt opgebouwd uit volgende onderdelen:

- 2x sluisdeur onderdeel
- 1x scheepvaartsein onderdeel per sluisdeur onderdeel
- 1x ricketschuif onderdeel per sluisdeur onderdeel
- 1x noodstop onderdeel
- 1x logische uitwerking

5 Werking model



Het gemaakte model representeert de bediening van een schutsluis. Hierbij is gebruik gemaakt van bovengenoemde onderdelen om dat te realiseren. Het model representeert een schutprocess waarbij alleen de bediening van de schutsluis is gemodelleerd. Om de bediening te kunnen modelleren is er gebruik gemaakt van schepen in de vorm van getallen die continue verhoogt of verlaagt worden.
Het begin punt van het model is:

- Gesloten sluisdeuren
- Scheepvaartseinen in de toestand 'Rood'
- Gesloten ricketschuiven
- Noodstop is beschikbaar om ingedrukt te worden

Na dit moment zal het model autonoom werken waarbij de simulatie process uitgeschreven in hoofdstuk *Specificaties* doorgelopen wordt.

6 Geverifieeerde eigenschappen

Requirements	Geverifieeerd	Formule
Sluisdeuren 1 (veiligheig)	PASSED	E<> not (D9.Open and D0.Open))
Sluisdeuren 2 (veiligheid / bereikbaarheid)	PASSED	A<> not (H1.Open and L1.x¿=level_timer) and D1.Closed A<> not (H0.Open and L1.x¿=level_timer) and D0.Closed
Sluisdeuren 3 (veiligheid)	PASSED	A<> not ((D0.Opening or D0.Closing) and S0.Green)
Sluisdeuren 4 (veiligheid)	PASSED	A<> (H0.Open and L1.x¡=level_timer) imply (D0.Closed and D1.Closed and S0.Red and S1.Red)
Ricketschuiven 1 (veiligheid)	PASSED	E<> not (H0.Open and H1.Open)
Ricketschuiven 2 (veiligheid)	PASSED	A<> (H0.Open imply not D1.Open) and (H1.Open imply not D0.Open)
Scheepvaartseinen 1 (veiligheid)	PASSED	A<> (S0.Green imply not S1.Green) and (S1.Green imply S0.Green)
Scheepvaartseinen 2 (veiligheid)	PASSED	A<> (S0.Green imply (not (D0.Opening or D0.Closed or D0.Closing)))
Noodstop 1 (veiligheid / fairness)	PASSED	A<> Emergency.Ready
Noodstop 2 (veiligheid)	FAILED	-
Noodstop 3 (veiligheid)	PASSED	Noodstop 1
Noodstop 4 (veiligheid)	FAILED	-
Noodstop 5 (veiligheid)	PASSED	A<> Emergency.Stopped imply (H0.Closing or H0.Closed)
Noodstop 6 (veiligheid)	PASSED	A<> Emergency.Ready imply (H0.Closed and H1.Closed)
Noodstop 7 (veiligheid)	PASSED	A<> Emergency.Stopped imply (S1.Red_Red and S0.Red_Red)

Referenties

[1] Julianasluis 2 bedienininstructie. 2014.

[2] Edmund M. Clarke, Jr., Orna Grumberg, and Doron A. Peled. *Model Checking*. MIT Press, Cambridge, MA, USA, 1999.

[3] R.J de Vries. Algemene elektrotechnische voorschriften bruggen en sluizen. 2014.

[4] A. Vrijburcht. *Ontwerpen van schutsluizen*. Rijskwaterstaat Bouwdienst, 2000.