Report System Validation Project
Modeling a Bridge's Control System
Creating a safety layer with mCRL2 using Labelled Transition Systems

Aimee Ferouge 4014030
Wieger IJntema 4034570
Arian Stolwijk 4001079
Group 7

December 18, 2013

Date Performed: Januari, 2013
Instructor: J. J. A. Keiren

1 Preface

Contents

2 Summary

In this section we will summarize the project.

2.1 Introduction

As has been pointed out by the incident at the Ketelbrug between Emmeloord and Lelystad, bridges require a very precise control system. Many examples exist where bridges are not opened or closed properly, where bridge components break down or the bridge is being stuck in a particular state. The goal of this project is to design a safety layer that can be added to the main control interface, in order to capture all possible situations and failures. Throughout the report, we make use of the following assumptions:

- If three or four sensors detect an open/closed bridge, the bridge can be considered open/closed
- If only the four sensor have a 50/50 detection on the bridge deck, the bridge should remain in its current position (open/closed)

- A barrier can only be considered to be down when the majority of the sensors detect a lowered barrier

In this section, the desired behaviour of the bridge is being determined and defined. Section 1.3 contains the global requirements that will be met in our system. Specific interactions that can be performed by the bridge are discussed in Section 1.4, whereas Section 1.5 translates these interactions into the requirements stated earlier.

2.2 Global Requirements

Using the Project Guide[1] as a source for the desired behaviour, the following requirements are defined:

Opening the bridge

1. Stop signs cannot be lit unless the pre lights are lit
2. Barriers cannot be lowered unless the stop signs are on
3. Bridge can only be unlocked when all barriers are down
4. The deck can only lifted when both locks are unlocked

Closing the bridge

5. Bridge can only be locked when the deck is down
6. Barriers can only be raised when the bridge is locked by at least one lock

Functional requirements

7. The bridge should be able to be opened when a ship approaches
8. The bridge should be able to close and barriers should in order to let cars pass
9. The second barrier encountered by the cars is lowered after the first in order to enable cars to leave the bridge

Failure

10. The stop signs can only be lit if at least one pre sign is lit at each side of the bridge
11. The barriers can only be lowered if both stop signs are lit at each side of the bridge
12. If the motor is in the 'broken' status, the bridge may not be opened

2.3 Interactions

2.4 Architecture

Three parallel processes exist being *signs*, *barriers* and *bridge*. *Signs* handles the control of the lights, whereas *barriers* handles the barriers and *bridge* the locks and the deck.
Signs is the first one to be executed when an `open` or `close` command is given. After first lighting the pre signs and then the stop signs, control is given to the *barriers* process.
Barriers makes sure all barriers are lowered if the stop signs are lit. When this is the case, *bridge* takes over.

[1] J. J. A. Keiren, System Validation (IN4387) Project Guide, VU University Amterdam, november 2013

Interaction	Descripton	Parameters
`open`	Opens the bridge	
`close`	Closes the bridge	
`getSign`	Checks te status of a specific sign	Sign
`setSign`	Switches a sign on or off	Sign, status
`getBarrier`	Checks the status of a specific barrier	Barrier
`setBarrier`	Lowers of lifts a specific barrier	Barrier, status
`getLock`	Checks the status of a specific locking pin	Lock
`setLock`	Locks or unlocks a specific locking pin	Lock, status
`getDeck`	Checks the status of the bridge deck	
`setDeck`	Lowers or liftst the bridge deck	Status
`motorStatus`	Checks the status of the motor	

Table 1: All interactions to be performed by the safety layer of the control system.

Bridge handles the lifting and lowering of the bridge deck. Only when all barriers are down, the two locks of the bridge are removed and the deck can be moved up and down. When finishing this movement, control is given back first to *barriers* and finally back to *barriers*.
Figure 1 shows a sequence diagram of how the control shifts between these parallel processes.
n

2.5 Translation of Requirements in Terms of Interactions

In order to create a model for the bridge in mCRL2, which is modeling software used for system validation, the requirements have to expressed in terms of the previous stated interactions. At the moment, we are still rewriting these translations after the feedback we received during last week's meeting. The following translations are from last week.

1. **Stop signs cannot be lit as long as the pre lights have not been lit** When setSign(Si,On), before setSign(Pi,On) should have occurred and setSign(Pi,Off) may not occur intermediate.

2. **Barriers cannot be closed if the stop signs have not been lit** When setBarrier(Bi,Up), before setSign(Si,On) should have occurred and setSign(Si,Off) may not occur intermediate.

3. **Bridge can only be unlocked when all barriers are down** When setLock is set unlocked for all locks, then check for all barriers if getBarrier is down before, and not up intermediate. Else, give error and stop.

4. **The deck can only lifted when it is completely unlocked** When setDeck is set up for the bridge deck, then check for all locks if getLock is unlocked before, and not locked intermediate. Else, give error and stop.

5. **Bridge can only be locked when the deck is down** Always when setLock(L2), then getDeck is down before, and not changed intermediately. Always when setLock(L1), then getDeck is down before, and not changed intermediately.

6. **Barriers can only be up when the bridge is locked by at least one lock** Always when setBarrier(B, up), getLock(L1) or getLock(L2) are enabled, and not disabled intermediately.

7. **Stop sign can be shut off only when the barriers are up** Always when setSign(S_i, off) occurs, setBarrier(B_i, up) has to be occured before for all barriers. No setBarrier(B_i, down) may have occured intermediately.

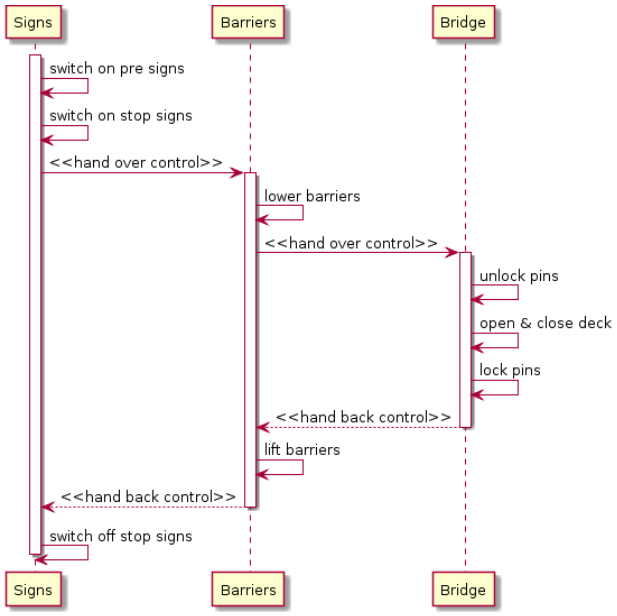

Figure 1: Sequence diagram of control flow between parallel processes *signs*, *barriers* and *bridge*.

8. **The bridge should be able to be opened when a ship approaches** When open occurs, setDeck(OPEN) should eventually occur.

9. **The bridge should be able to close in order to let cars pass** When close occurs, setDeck(CLOSE) should eventually occur.

10. **The first barrier to be encountered by the cars is lowered earlier than the second in order to enable cars to leave the bridge** Always when setBarrier(B_2, down), setBarrier(B_1, up) has to be occured before. No setBarrier(B_1, up) may have occured intermediately. Always when setBarrier(B3, down), setBarrier(B_4, up) has to be occured before. No setBarrier(B_4, up) may have occured intermediately.

11. **The stop signs can only be lit if at least one pre signs is being lit at each side of the bridge** Always when setSign(S_1, on) or setSign(S2, on), at least one status of getSign(P1) or getSign(P2) must be on. If not, the process is stopped. Always when setSign(S1, on) or setSign(S2, on), at least one status of getSign(P1) or getSign(P2) must be on. If not, the process is stopped.

12. **The barriers can only be lowered if both stop signs are being lit at each side of the bridge** Always when setBarrier(B1, down), getSign(S1) and getSign(S2) must be down. If not, the process is stopped. Always when setBarrier(B1, down), getSign(S1) and getSign(S2) must be down. If not, the process is stopped.

13. **If the motor is in the 'broken' status, the bridge should stay in the current position** Whenever motorStatus has been changed to broken and has not changed back to stopped, moving up or moving down, no components may be set anymore.