System validation, 2IW26

Jan Friso Groote (J.F.Groote@tue.nl, MF 7.070), Julien Schmaltz (J.Schmaltz@tue.nl, MF 7.071b).
http://www.win.tue.nl/~jfg/educ/2IW26/herfst2014/overzicht.html

The purpose of this course is to learn how to specify behaviour of systems and to experience the design of a system where you can prove that the behaviour is correct. So, you will learn how to formally specify requirements and to prove (or disprove) them on the behaviour. With a practical assignment you will experience how to apply the techniques.

The lectures are mainly dedicated to learn the foundations of the specification language mCRL2 and to use it as a manual specification and verification tool. There will be 2x2 hours of lectures per week, on Wednesdays 1/2 and Fridays 7/8.

In parallel to the lectures there will be an assignment, which must be finished before the examination period at the end of the semester. The goal of the assignment is to apply the techniques and tools to the design of a small distributed and/or embedded system. The purpose is to design this system such that it is proven to comply with all the requirements which must have been formulated in advance.

The marks for the exam and the assignment contribute equally to the final score. The final mark is the average rounded to a whole number in the ordinary way (7.5 is rounded up to an 8, 7.49 is rounded down). The mark of the resit of the exam will consist for 50% out of the result of the assignment and for the other half of the result of the exam. The result of the assignment is only valid for one year. If the course is redone in a subsequent year, the assignment must be done again.

Literature

The course material consists of

- J.F. Groote and M.R. Mousavi. Modeling and analysis of communicating systems. MIT Press, 2014. Chapters 1, 2 (not 2.3.2, 2.3.3, 2.4.4), 3, 4, 5 (not 5.6), 6, 7, 9 (not 9.7 and 9.8.3), 10, 11.
- See www.mcrl2.org for the tools, manual pages etc.

At http://ocw.tudelft.nl/courses/computerscience/systemvalidation/course-home/ the first five chapters of the book can be found. Note that the book contains an appendix with answers to exercises. The exam will cover the indicated parts of the book as well as everything said during the lectures.

Assignment

The assignment consists of designing a controller for a small distributed and/or embedded system. Below a suggestion for such a system can be found. It regards the adaptation of the Dutch automatic train protection system to the advent of the ERTMS (European Railway Traffic Management System) system. But it is possible to design any embedded controller or distributed algorithm provided you obtain approval by the supervisor of your assignment. The assignment can be carried out in groups of one to four persons.

Carrying out the assignment consists of executing the following steps:

1. Identify in words global requirements for the whole system. Typical requirements are ‘a bridge will never open when the barriers are not closed’. These requirements are initially to be described in natural language.
2. Identify the interactions that are relevant to your system. Describe clearly but compactly the meaning of each interaction in words.
3. Translate the global requirements in terms of these interactions.

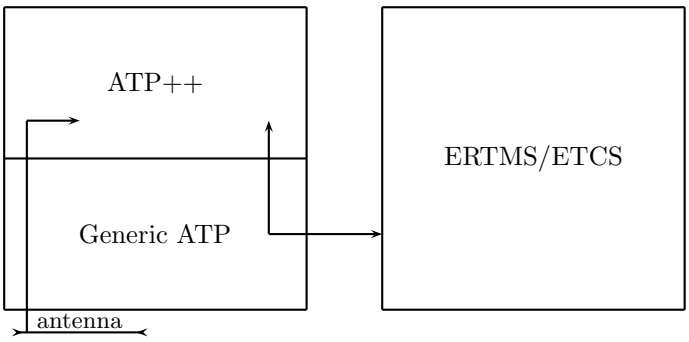

Figure 1: Schematic overview of the new ATP system

4. Describe a compact architecture of the structure of the system. It is required that the controller has at least three different parallel components.

5. Describe the behaviour of all controllers in the architecture using mCRL2.

6. Verify using the toolset that all requirements given in item 3 above are valid for the design in mCRL2.

The assignment must be documented in a technical report that covers all items above. This report must be a concise technical account of the system and must be written such that from it the requirements, action interface, architecture and behavioural design can be easily understood. It must also be clear how the requirements are verified, in such a way that this can easily be redone exactly without consulting any of the authors of the report. So, for instance the exact commands that are used must be listed, it must be obvious which version of the toolset was used for the verification and on which platform and operating system the verification was done.

The new ERTMS (European Railway Traffic Management System) system is destined to become the standard control system for all trains in Europe. The task of the ERTMS system is essentially to allow that trains can safely drive over the tracks. Currently, each country has its own train control mechanisms, which is causing problems for inter-state train traffic.

Currently most European countries use their own safety guarding system, called Automatic Train Protection (ATP, in Dutch: Automatische Treinbeïnvloeding, ATB). Each country has its own variant. This system works by putting a pulse shaped electrical signal on the track. This generates an electrical field which is detected by an antenna at the front of the train. The higher the frequency of the pulses, the faster the train is allowed to drive. The Dutch system is such that if there are no pulses, the train is still allowed to drive with a speed up to 40km/h. This is done to avoid that trains come to a halt due to the system malfunctioning. The other speed limits are 60km/h, 80km/h, 130km/h and 140km/h. There is one special pulse frequency, indicating that the ATP should be switched off. This is used for remote and hardly used lines where trains should still be able to drive with speeds over 40km/h.

If a train drives with a speed higher than the speed allowed by the ATP, then the cabin bell will sound. If the train driver does not react within three seconds the ATP will automatically employ the emergency brakes. The train will then come to a full stop. After the train has stopped, the train driver can reset the ATP and continue driving.

There is a problem with the ATP system for freight trains. The brakes of freight trains have a tendency to release slowly. So, after releasing the brake, the train will still slow down substantially, before the brakes are off. This means that the speed of the train becomes lower than necessary, and a

lot of energy is required to get a train back to speed. It can even result in a premature and unwanted stop of these trains. If a heavy freight train stops on an upward slope, the locomotive cannot put the train into motion again. In such a case an extra locomotive must be arranged, or the train must be split and tugged away in parts. This is time consuming and disruptive for the other train traffic. Therefore, if a train is braking and the allowed speed of the ATP is not yet reached, the train driver is at some point already allowed to release the brakes (indicated by a bell ringing three times). In this case the ATP will not go into emergency braking.

A recent addition of the Dutch ATP system is ATB-vv (ATB verbeterde versie, ATB improved version). This system works independently of the basic ATP system. This system has been developed because it turned out that too often a train driver passed a red signal with a speed below 40km/h. This system is specially designed to stop trains driving past red signals with low speed. It consists of a number of beacons besides the track that send stop messages when the stop signal is red. If a train is driving at low speed, it will automatically stop before the signal. If a train is driving a high speed, it may stop past the signal. Note that ATB-vv is not fail safe. If the beacons erroneously do not send a signal, the train will not come to a stop.

When introducing the ERTMS/ETCS system, it will take over the safety functionality of the ATP systems. But for a number of years both systems will operate simultaneously. Therefore, the ATP system must be adapted, because it does not have direct control anymore over the user interface and brakes and cannot measure the speed of the train directly. The new ATP must control these via the ERTMS. The new situation is depicted in figure **??**. In order to make the system usable with small modification for all European ATP systems, the new ATP system is split in a generic and a country specific part. The generic part is responsible for the communication with the ERTMS/ETCS system and deals with reading the signal from the antenna. The country specific part is called ATP++ and it implements the particular country dependent rules that apply.

There is a special situation which should be dealt with, which occurs when the train leaves or enters ATP protect tracks from/in ERTMS protected tracks. When it enters ERTMS protected tracks, the antenna does not receive any signal anymore, and if not properly switched off, the ATP will instruct the ERTMS system to bring the train to a halt if the train drives with a speed above 40km/h. If an ERTMS protected track is left, and the ATP is not properly switched on, the train may drive non safeguarded, undoubtedly leading to accidents. What complicates matters is that if either ERTMS or ATP is in a specific mode (e.g., about to instruct an emergency braking), then this mode should be taken over by the other system. Unsafe situations should never occur, especially not when entering or leaving an ATP protected area.

The request is to model the new ATP++ and generic ATP system. It should include the old functionality of the ATP and it might contain the functionality of the ATP-vv extension. The ATP++ and generic ATP must be modelled as independent parallel components. For the purpose of this assignment, the ATP++ system must consist of at least two parallel components. The description above will turn out to be rather vague if the behaviour of the system is modelled. When this happens you are allowed (even stimulated) to choose your own view on the system even if it is not in accordance with the description above as long as you can defend your choice. One of the reasons for this is that the time to accomplish this assignment is rather short. You should not be delayed by awaiting a verdict from the teachers of this course but resolve modelling and design choices yourself.

Tool set

See `www.mcrl2.org` and the webpage of the course.

Global time schedule

Below a global time schedule is indicated. There are exercises indicated, which upon request can be treated during the lectures. Students are supposed to make these exercises before the lectures, and

compare their answers with those of the lecturer. The exercises can be found in the reader. Short answers are provided in appendix F.

3/5-9-2014. Chapter 1. Chapter 2. Chapter 4. Transition systems, basic processes, process equivalences, conditional operator, time. Elementary reasoning with axioms. The toolset and its philosophy. Exercises 2.2.2, 2.2.3, 2.3.2, 2.3.8, 2.3.9, 2.3.10, 2.4.6, 2.4.7 4.2.3, 4.2.4, 4.3.1, 4.3.2, 4.4.1, 4.5.1, 4.5.2.

10/12-9-2014. Chapter 3. Chapter 4. Section 9.4. Appendix B. Abstract data types. Constructors. Built in data types, bool, quantifiers, pos, nat, int, real. list, set, bag, functions, structured type. Difference between $\approx$ and $=$. Predefined data types, induction. Exercise 3.1.2, 3.1.3, 3.1.4, 3.2.2, 3.2.5, 3.2.6, 3.3.3, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 3.6.1.

17/19-2-2014. Section 4.6. Chapter 5. Section 9.6. Recursion. RSP. Proving recursive specifications equal. Parallel processes and hiding. Expansion law. Communication, multi-actions. Exercises. 4.6.1, 4.7.1, 4.7.2, 4.8.1, 5.1.1, 5.2.1, 5.4.1, 9.6.4, 9.6.5, 9.6.6, 9.6.9.

24/26-2-2014. Chapter 6. The modal μ-calculus with data. Exercise 6.1.2, 6.2.1, 6.3.1, 6.3.2, 6.4.1, 6.4.2, 6.5.1, 6.5.2, 6.5.3.

1/3-10-2014. Chapter 9. Sketch of the lambda calculus. Sum axioms. Sum elimination theorem. Precise proof system. Exercise 9.4.2, 9.4.3, 9.5.1, 9.5.2, 9.5.4, 9.5.5.

8/10-10-2014. Chapter 10. Linearisation of processes. CL-RSP, CL-RSP with invariants. Exercise 10.1.4, 10.2.9, 10.2.10, 10.2.11.

15/17-10-2014. Chapter 11. Confluence and τ-priorisation. Exercise 11.1.3, 11.1.4, 11.2.6.

22/24-10-2014. Reserve.

3-11-2014. Exam (13:30-16:30). Closing date for registration: 19-10-2014.

24-10-2014. Last date to hand in the pre-final report for the assignment. The report must be handed in on paper.

10-11-2014. Last date to hand in the final report for the assignment. The report must be handed in on paper and must be accompanied with the corrected pre-final report.

30-1-2015. Exam (resit, 13:30-16:30). Closing date for registration: 11-1-2015.