Prof. Dr. A. Podelski, Dr. B. Westphal
L. Musliu

Wintersemester 2017/18

Real-Time Systems

http://swt.informatik.uni-freiburg.de/teaching/WS2017-18/rtsys

Exercise Sheet 4

Early submission: Monday, 2017-12-04, 14:00 Regular submission: Tuesday, 2017-12-05, 14:00

Exercise 1 (4/20 Points)

Consider the interpretation of P as shown in the timing diagram in Figure 1.

- Describe the set of interpretations of R such that

  $$\lceil R \rceil \longrightarrow \lceil P \rceil$$

  holds on the interval $[0, 8]$.

  What is the shortest accumulated duration of $R = 1$ in these interpretations? Does a shortest duration exist? (2)

- Describe the set of interpretations of Q such that

  $$\lceil P \rceil \xrightarrow{2.5} \lceil Q \rceil$$

  holds on the interval $[0, 8]$.

  What is the shortest accumulated duration of $Q = 1$ in these interpretations? Does a shortest duration exist? (2)

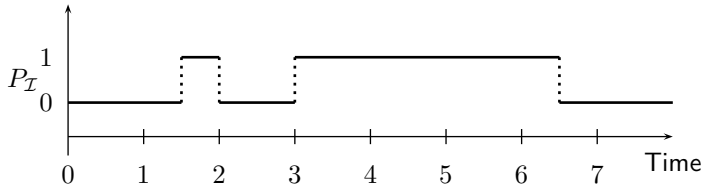

Figure 1: Timing diagram for Exercise 2.

Exercise 2 (4/20 Points)

Discuss the difference between the stability pattern

$$\lceil \neg\pi \rceil \,;\, \lceil \pi \rceil \xrightarrow{\leq\theta} \lceil \pi \rceil$$

and the standard form $\lceil \pi \rceil \xrightarrow{\leq\theta} \lceil \pi \rceil$. (For example, for $\pi = \mathsf{purge}$ (from the gas burner) and $\theta = 30$.)

In particular explain what $\lceil \pi \rceil \xrightarrow{\leq\theta} \lceil \pi \rceil$ does specify, that is, for which evolutions of C (= gas burner local state) does it hold and for which not?
Hint: Illustrate your discussion generously with examples.

Exercise 3 (12/20 Points + 5 Bonus)

Background Information

Wireless fire alarm systems (WFAS) are regulated by European Norm EN-54. Certificates of conformance with EN-54 for a WFAS can be obtained by submitting a WFAS system to a certification agency[1] where the system is tested according to procedures specified in EN-54. If the system passes all tests, the EN-54 conformance certificate is issued.[2]
Requirements of EN-54 for WFAS include properties like "a single alarm is displayed at the central unit within 10 s" and "a sensor malfunction is detected by the system within 300 s" (self-monitoring).
WFAS need to function reliably in particular in the presence of disturbances on the used radio frequency (e.g. caused by microwave ovens or other devices operating on the same frequency). Thus the certification agency conducts the tests in the presence of a *jamming device*, a device which, following certain constraints, non-deterministically emits noise on the relevant frequencies.

Task

The jamming device has to satisfy the following constraints:

(R0) There are exactly four different frequency bands A, B, C, D to be affected.

(R1) At each point in time, at most one of the frequency bands is "jammed".

(R2) Jamming phases last for at least $1\,s$.

(R3) When changing the frequency to be jammed, all radio frequencies are free for at most $1\,s$.

(i) Formalise the requirements using DC. (2)

Hint: (R0) and (R1) can be treated by a good choice (and explanation) of observables.

(ii) Provide a controller design for the jamming device using implementables. (7)

Provide a convincing and elaborate description of your design, including arguments why it is correct. Some natural questions are: What is your exact understanding of the requirements? Why did you choose which control states? Why is this a good choice? What does each implementable contribute to the overall controller behaviour? etc.

In particular discuss the aspect of reaction time; an arbitrarily slow hardware platform may not be able to deliver the required evolutions.

Hint: You need not explicitly provide control automata for the actuators, i.e. for jamming of the channels; just describe how the actuator behaviour relates to the local states of your controller.

(iii) Demonstrate that your controller design is not "completely broken" by providing one evolution which realises requirements (R1) to (R3) (under assumption (A1)) and, for (R2) and (R3), one evolution which does not realise exactly that constraint; explain why the former evolution is in the set of evolutions described by your system of control automata, and why the latter two are not. (3)

(iv) Prove that your controller design is correct wrt. (R1) to (R3). (5 Bonus)

[1] in Germany, e.g., the VdS (Verband der Sachversicherer / Vertrauen durch Sicherheit) in Köln.

[2] To conclude a fire insurance contract for certain objects, insurance companies usually require that an EN-54 conforming fire alarm system is installed in the object; hence developers of "serious" fire alarm systems have a strong interest in obtaining an EN-54 conformance certificate.