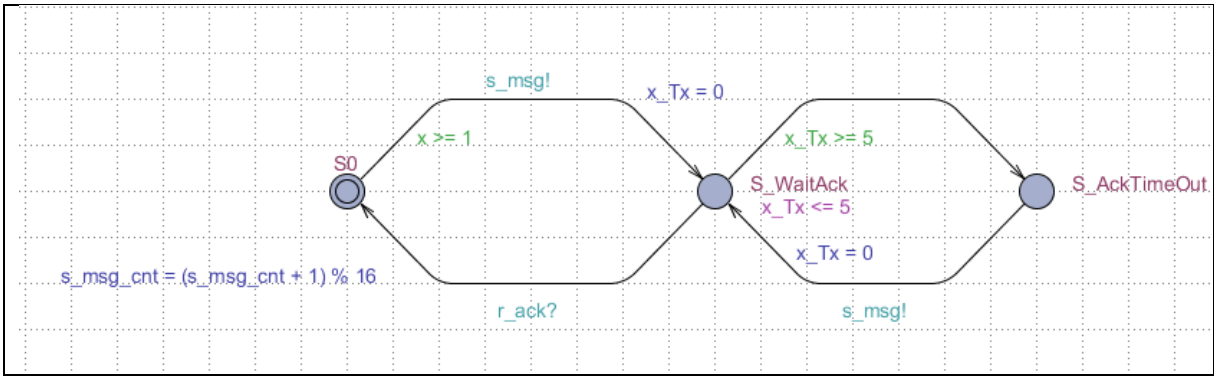
Report on Assignment 4, "Model Checking of Real-Time Systems"

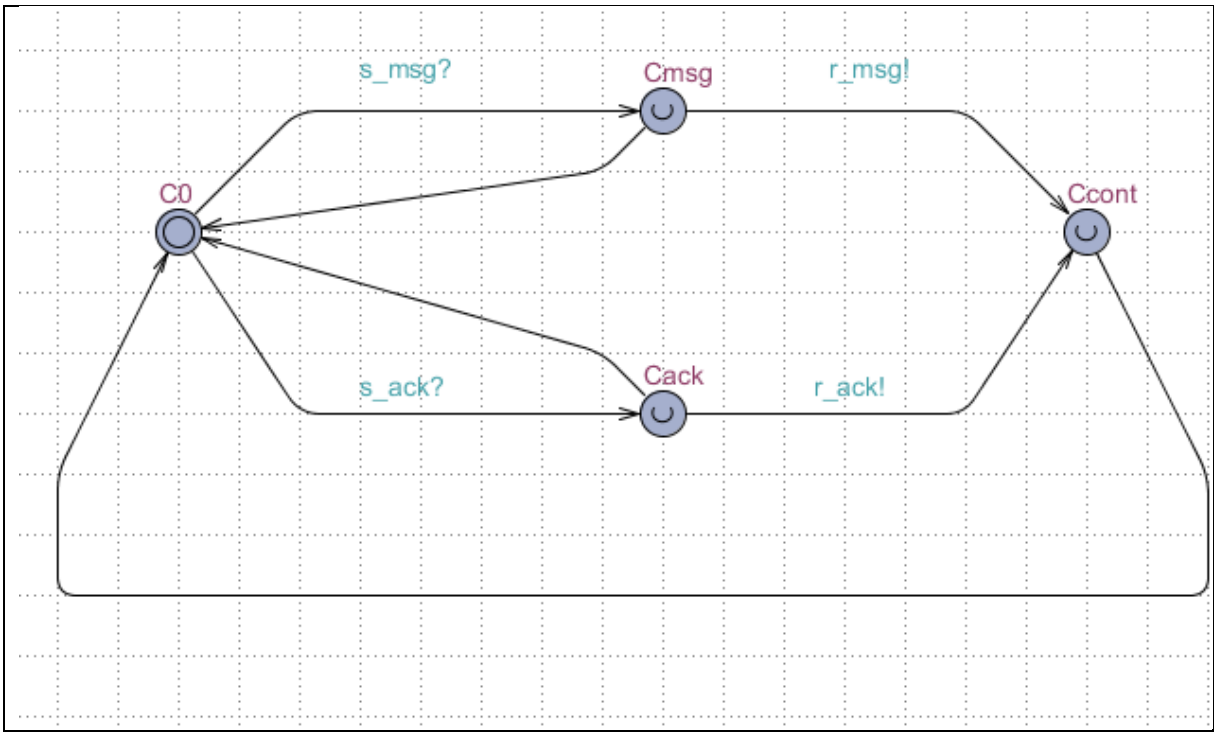
The system is modelled in UPPAAL as indicated in figures below:

Sender:



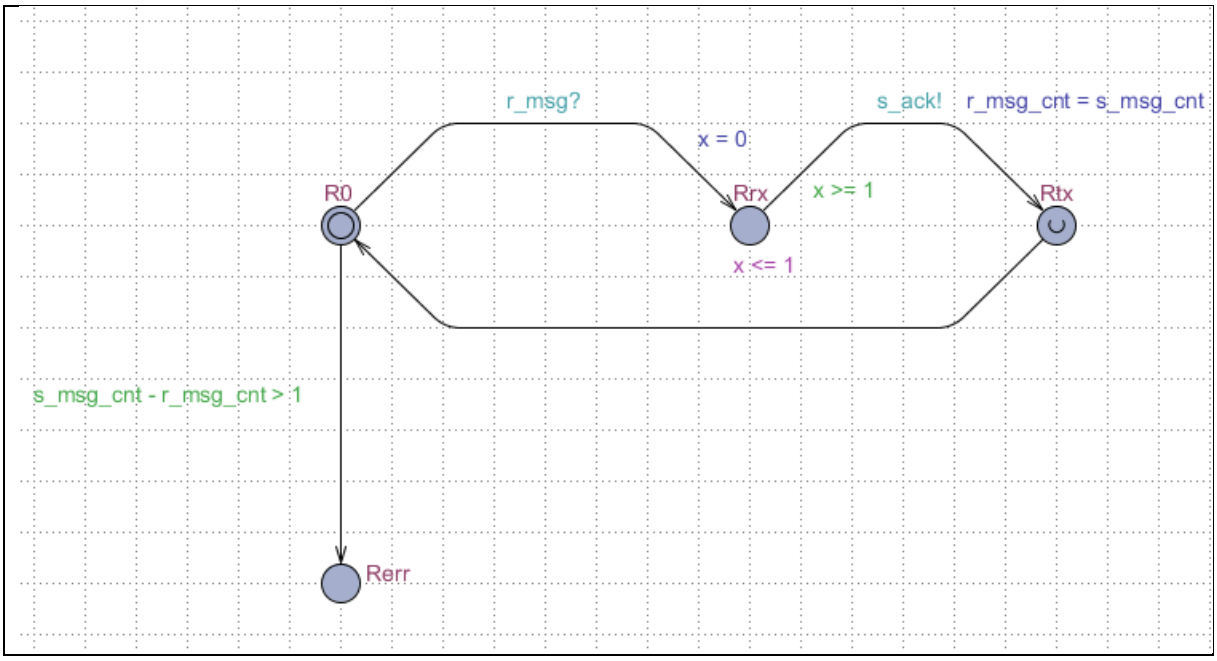
The Sender continuously sends s_msg:s and wait for then to be acknowledged, if the wait is above 5 time units a retry is made. The retries are made until the message has been acknowledged. Th Sender keep track of number of messages acknowledged, this is used at the receiver to detect any missed message – see notes below!

Channel:



The Channel just copies the received **s_msg** to the output **r_msg**, at the same time it does the same for any **s_ack** which are output as **r_ack**. It is possible that such an output fails, thus nothing is sent out!

Receiver:



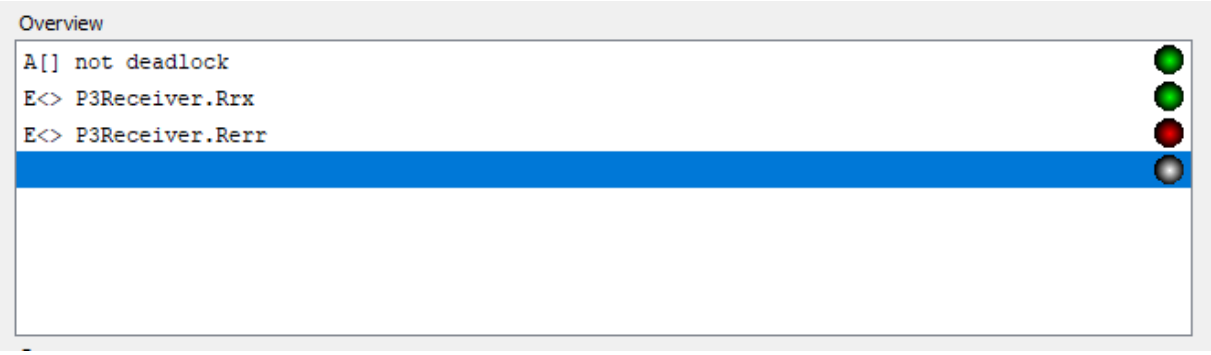
The Receiver takes in any **r_msg** and confirms this with an output of an **s_ack** back to the Channel. It takes one time unit to send the **s_ack.** The Receiver keeps track that no message sent from the Sender is lost, if such a loss is detected the system is terminated to an error state **Rerr**.

Verification

Three different verifications are required:

- The system cannot deadlock;
- The receiver might send an acknowledgment;
- The messages sent by the sender are eventually received by the receiver.

This is done in UPPAAL with:



The first line indicates that there is no dead lock.

The second line indicates that the Receiver is sending an acknowledgement

The third line indicates that it is not possible to reach the error state Rerr, thus no messages have been missed.

Ref. Files `DVA404_A4_gfm10001_v2.q` and `DVA404_A4_gfm10001_v2.xml`