

CSSE 373 - Formal Methods in Spec. and Design

Verification of the Reliable Data Transfer Protocol

You will apply your modeling and verification skills to an important real world problem as a part of this project. This project will run for three weeks and has three sprints. You will work with your teammates on this project. You will incrementally verify the Reliable Data Transfer (RDT) protocol explained in the hand-out given to you.

Assumption

Please make the following assumption to start with:

1. The data transfer happens between one sender and one receiver only.
2. Both sender and receiver have their own buffer that can hold a **set** of data.
3. A transfer is reliably completed if the receiver buffer eventually receives all of the data initially present in the sender's buffer.

Note that you may have to make more assumption based on the version of RDT you are modeling.

Project Plan

The project is divided into three sprints, each running for a week. In each sprint, you will check the following two properties of the protocol you are modeling:

1. Using the given protocol, it is possible to transmit all of the data in the sender's buffer to the receiver's buffer. Here, you are asked to find one possible way to do so.
2. Using the given protocol, it is **always** possible to transmit all of the data in the sender's buffer to the receiver buffer. Here, you are asked to find one possible way in which the data **cannot** be transferred, thus, refuting the claim. You must ensure that the causes of flaws are due to the flaws in the protocol and not your model. Keep in mind that **not** all versions of RDT have flaws.

Sprint 1 – Checking RDT 1.0

Due: May 4, 2015, 8:00 AM

Model RDT 1.0 with the specification given in the hand-out [name it **RDT10.als**]. Create a report [name it **RDT10.pdf**] that either shows violation or conformance of the two properties. You must show snapshot of traces with explanation where applicable. Turn in **RDT10.als** and **RDT10.pdf** on Moodle (One submission per team). [5 points]

Sprint 2 – Checking RDT 2.0

Due: May 11, 2015, 8:00 AM

Same description as Sprint 1 but you will model RDT 2.0 in this sprint. Turn in **RDT20.als** and **RDT20.pdf** on Moodle. [10 points]

Sprint 3 – Checking RDT 2.1

Due: May 18, 2015, 8:00 AM

Same description as Sprint 1 but you will model RDT 2.1 in this sprint. Turn in **RDT21.als** and **RDT21.pdf** on Moodle. [5 points]

Extra Work for Three-Membered Teams: The teams with three members must also model RDT 2.2 and turn in **RDT22.als** and **RDT22.pdf** in this sprint.

Grading Policy

The project contributes 20% to your final course grade. Towards the end of the last sprint, there will be a **peer evaluation** of individual contribution on the project that will be used to scale the individual grade.