

SWS assignments:

Computer-controlled Kart Racing 2

Critical examination



Assignment for Team A:

Change in software control basics

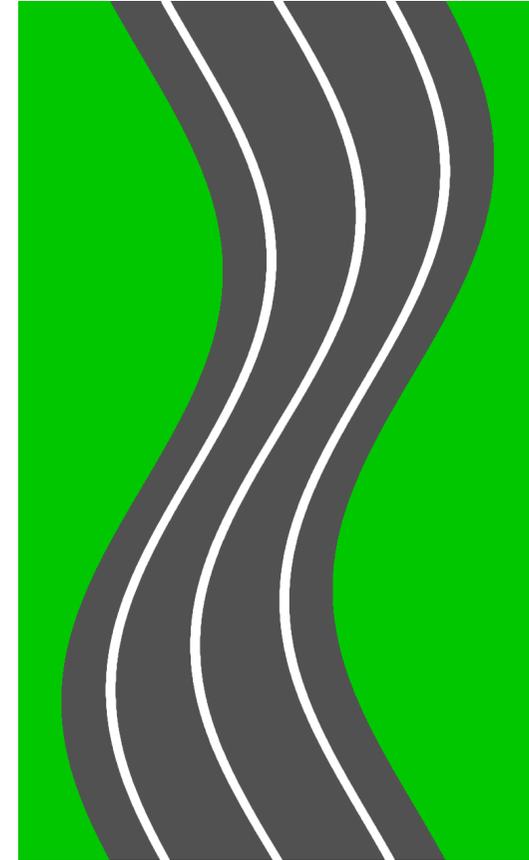
In the original plan, karts would only change lanes in response to a driver “request”; never because of software intervention.

But once a kart is stopped behind another stopped kart, it can't change lanes anymore and must wait for the other kart to start moving again. Experiments have shown that this happens often, detracting from the fun. Management has now decided that karts should also change lanes if needed to keep a kart from getting stuck — of course only if safe.

- Can the safety specs as developed by each of the teams be adapted to accommodate this change? Discuss critically how easy or difficult the adaptations are.

Assignment for Team B: Chicanes

In the original plan, karts would never need to slow down if there is no kart ahead in the same lane. Management has now decided to introduce track-narrowing chicanes in the circuit, which means that karts may need to slow down to avoid crashing into a kart in the next lane (see image).



- Can the safety specs as developed by each of the teams be adapted to accommodate this change? Discuss critically how easy or difficult the adaptations are.

Assignment for Team C:

Can the control loop ensure safety?

Recall the software control loop as described in the assignment for Slot 7, and the assumptions stated there.

Question: Is it possible to define (or specify) a control loop as described that is provably safe *using the notion of safety as specified by the teams*, because (under the assumptions) the loop will keep the system in a safe state as a system invariant.

- Give a reasoned answer to this question for each of the specs.
 - If the answer is yes, how? Sketch the proof.
 - If the answer is no, why not? What needs to be improved?