

Exam test

UML for Embedded Systems

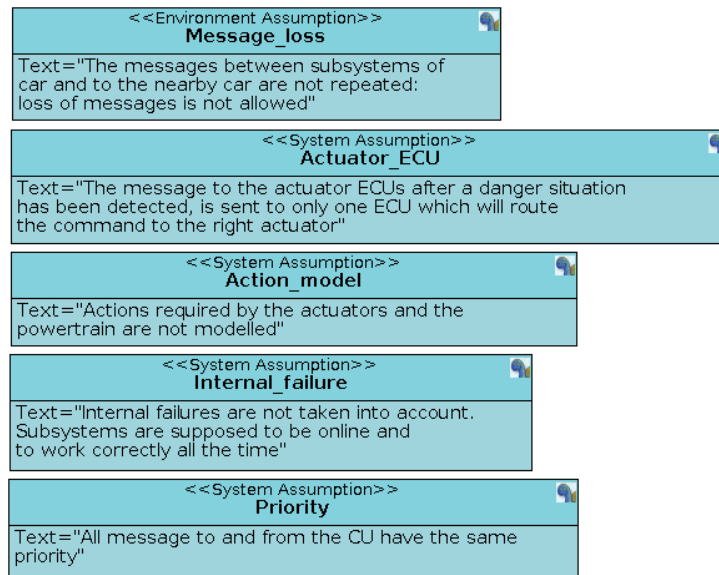
Simone ROSSI

November 21, 2016

Date Performed: November 21, 2016

Partners: Simone Rossi

1 Assumptions



2 Formal verification

For the formal verification, I checked that in all dangerous situations a broadcast message is sent to the nearby cars. To do that, I proved the reachability and the liveness property of the "message broadcast send" action in the CU are guaranteed.

The formal verification confirmed that these two properties are verified; this means that a message is always sent whenever a dangerous situation has been detected.

Moreover, I checked that the maximum time delay from the moment in which a dangerous situation has occurred and a broadcast message is sent is not more than 150 ms. To do that, I introduced an observer to between the **Sensor Chassis ECU** and the CU. Using a timer, I formally proved that the message is sent within 150 ms (e.g. the timer never expires and that state is never reachable).

Reachability of: CU.Send signal: broadcast(message)
-> property is satisfied

Reachability of: OBS_TimeDelay.State: TIMEOUT_ERROR
-> property is NOT satisfied

Liveness of: CU.Send signal: broadcast(message)
-> property is satisfied

Liveness of: OBS_TimeDelay.State: TIMEOUT_ERROR
-> property is NOT satisfied