1 Introduction

Hier komt een korte introductie.

2 System description

Each locomobile has:

- 3 motors
- 3 oil pressure pumps (1 per motor/engine)
- 3 position sensors

The output commands are:

- start motor N inward/outward
- start oil pump N
- stop motorn N inward/outward
- stop oil pump N
- stopped moving
- started fine-positioning
- sensor error N
- motor error N
- open/close valves
- pump water out

The input messages are:

- close/open/stop locomobile (received twice)
- position sensor N
- motor N was repaired

The locomobiles communicate with the central system called ‘BesW’

3 Global requirements

- One of the two channels is redundant so that every command is received twice.
- The sensors measure the same thing, so 2 of them are also redundant.
- When the 'open locomobile' command is received while the door is closed, the system shall open the door.
- When the door is opened, the system shall start fine-positioning and report 'started fine-positioning'.
- While the door is filled with water or the valves are open, the system shall not open the door.
- When the 'stop locomobile' command is received while the door is moving, the system shall stop moving the door within 10 seconds.
- When the 'close locomobile' command is received while the door is open, the system shall close the door.
- When the door reaches the closed position after receiving the 'close locomobile' command, the system shall open the valves, start fine-positioning, and report 'stopped moving' and 'started fine-positioning'.
- The system shall use at most 1 motor while it is fine-positioning.
- When the door is further than 1 meter away from its desired position while fine-positioning, the system shall move the door back to the desired position.
- After the system starts an oil pump or motor, the system shall not start any other oil pump or motor within 3 seconds.
- When position sensor N has reported a different position than the other two position sensors for 3 seconds, the system shall report 'sensor error N'.
- When the system reports 'sensor error N' while another sensor is broken, the system shall stop all running motors and oil pumps.
- While at least 2 sensors are broken, the system shall not start any motor or oil pump.
- When none of the position sensors reports a different value within 10 seconds after starting motor N, the system shall report 'motor error N'.
- When the system reports 'motor error N', it shall not start motor N or oil pump N again until it receives 'motor N was repaired'.

4 Interactions

Beschrijving van interacties.

5 Architecture

Architectuur van het systeem.

6 Behaviour (mCRL2)

The behaviour of the system in mCRL2.

7 Verification

Verify using the toolset that all requirements given in item 3 above are valid for the design in mCRL2.