1 Introduction

The 'Maeslantkering' is a system designed to protect the harbour of Rotterdam against storms in the North Sea. Our task is to re-design the software of one of its components, namely the locomobile. Some high-level description of the system.

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

1. When a command is received once, it should be executed.
2. When a command is received twice, it should be executed only once.
3. The system shall use at most 1 motor while it is fine-positioning.
4. 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.
5. When the 'open locomobile' command is received while the door is closed, the system shall open the door.
6. When the door is opened, the system shall start fine-positioning and report 'started fine-positioning'.
7. When the 'stop locomobile' command is received while the door is moving, the system shall stop moving the door.
8. When the 'close locomobile' command is received while the door is open, the system shall close the door.
9. 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'.
10. After the system starts an oil pump or motor, the system shall not start any other oil pump or motor within 3 seconds.
11. 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'. Might change this to be non-parametric
12. When the system reports 'sensor error N' while another sensor is broken, the system shall stop all running motors and oil pumps. Might change this to be non-parametric
13. While at least 2 sensors are broken, the system shall not start any motor or oil pump.
14. When none of the position sensors reports a different value within 10 seconds after starting motor N, the system shall report 'motor error N'.
15. 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

Below is a list of all interactions, along with a description of their meaning.

- `open`: Open the door.
- `close`: Close the door.
- `stop`: Stop current action. This can mean one of two things:
  1. Stop moving the door, even when it is not in a final position.
  2. Stop fine-positioning.
- `finished`: The door is in position.
- `startFinePos`: Indicates that the locomobile has started fine-positioning.
- `errorSensor`: Indicates that the sensors need human intervention, because their values will not concur.
- `errorMotor`: Indicates that all three motors are malfunctioning and need human intervention.

5 Requirements with interactions

This is a reformulation of the requirements to include the interactions.

1.

6 Architecture

Architectuur van het systeem.

7 Behaviour (mCRL2)

The behaviour of the system in mCRL2.

8 Verification

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