CLEARSY
Safety Solutions Designer

Hackathon
JUL2025

AIX
LYON
PARIS
STRASBOURG

WWW.CLEARSY.COM

Airlock

Specifying and implementing a Voter

Thierry Lecomte
R&D Director

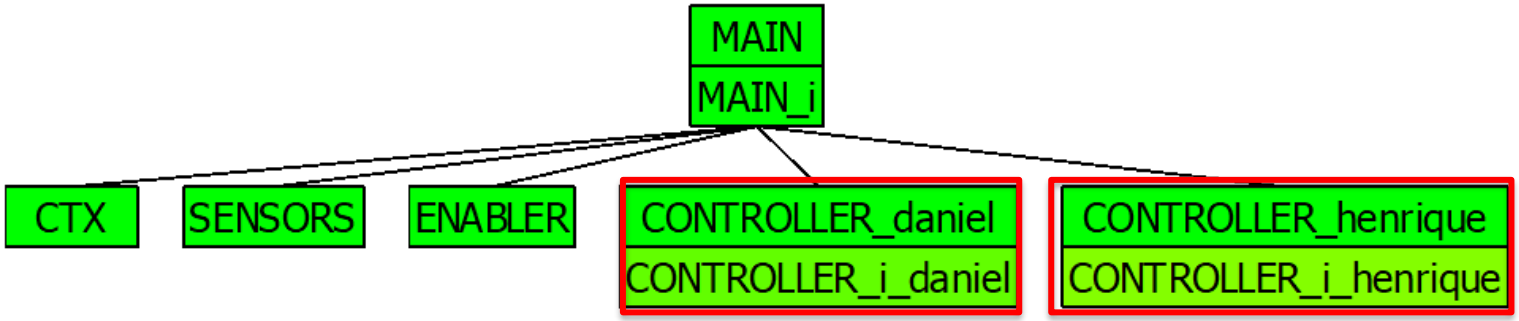
PART V

One Solution

THIERRY.LECOMTE@CLEARSY.COM

Your turn

- *Implement VOTER in MAIN_I [10 pt]*
  - *CONTROLLER duplicated (thank you Daniel and Henrique !)*



```
operate =
VAR act_d, auth_d, obj_d, act_h, auth_h, obj_h IN
    update_sensors_states;
    process_readers_daniel;
    process_readers_henrique;
    control_daniel;
    control_henrique;
    act_d, auth_d, obj_d <-- get_status_daniel;
    act_h, auth_h, obj_h <-- get_status_henrique;

    IF act_d = act_h & auth_d = auth_h & obj_d = obj_h THEN
        action := act_d
    ELSE
        action := NONE
    END
END
```

Your turn

- ***Optional**: What happens to the whole system if the controllers are functionally different? [1 pt]*

It gets stuck.

- *Optional: is it possible to adapt the voting principle to make it a bit more useful? [1 pt]*

Apply the voting only on opening door and modify pressure actions. Define recovery procedure. Complete the specification of the operation to get a proof that the functional behaviour is correct

The End

- ***Key facts***
  - ***How embedded systems are developed***
  - ***Hypotheses, safety architecture, specification, implementation***
  - ***Formal methods to help adding control***
  - ***Real systems are more complex:***
    - ***Situation is never 100% known***
    - ***Redundancy (sensors, actuators)***
    - ***Safety critical "IF THEN ELSE" could take 2k loc***
    - ***Human in the loop for maintenance operations***
    - ***Timing constraints***

And now the final results …