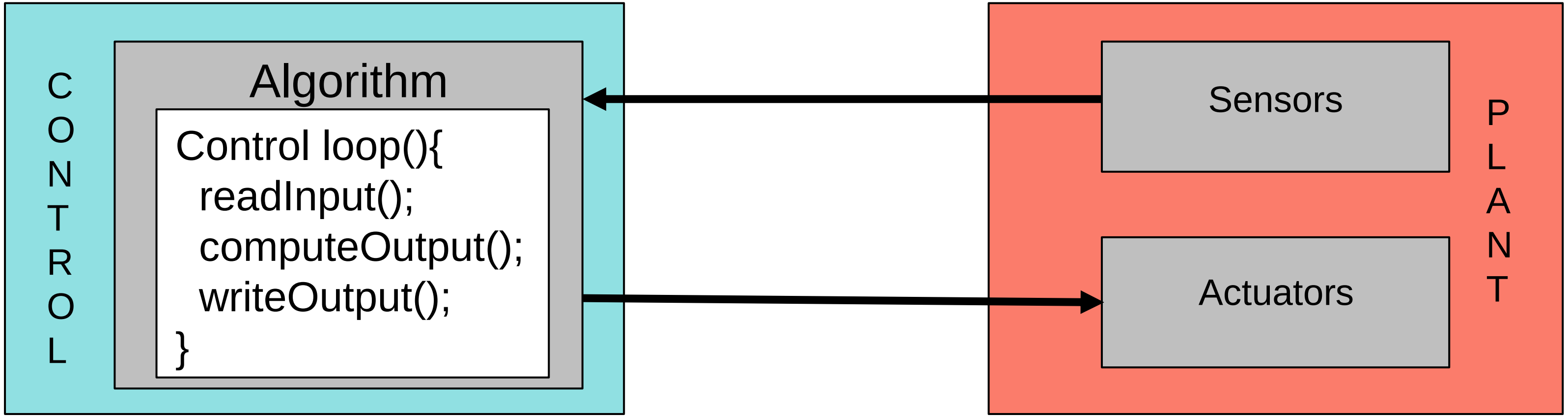
The road so far

Recap on attack analysis with co-simulation of CPSs

Attack analysis with formal methods

Connection between the two worlds

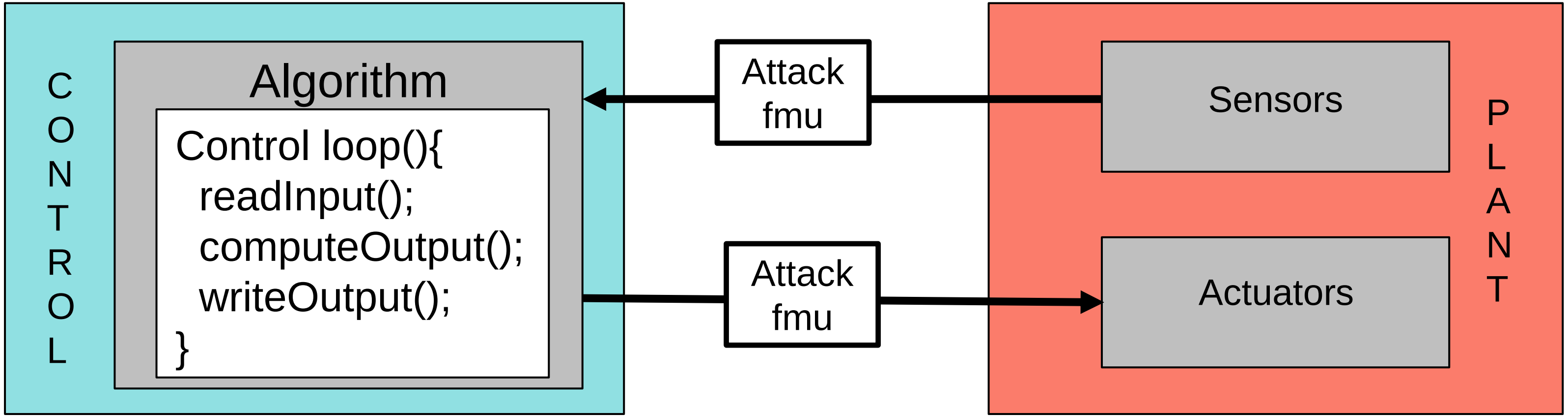
High level representation: Control + Plant



```
Control loop(){
  readInput();
  computeOutput();
  writeOutput();
}
```

In the case of the LFR the PLANT subsystem is composed of 3 different FMUs

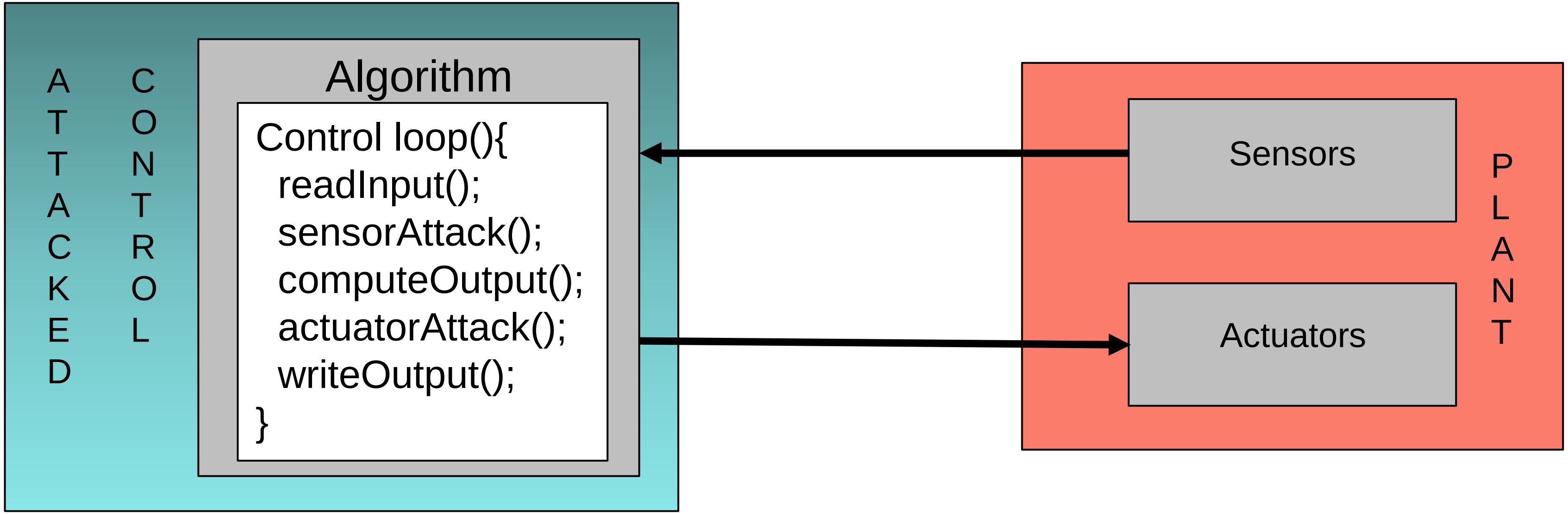
One way to implement attacks



```
Control loop(){
  readInput();
  computeOutput();
  writeOutput();
}
```

The behavior of the attack is implemented inside an external FMU added to the system

Another way to implement attacks



```
Control loop(){
  readInput();
  sensorAttack();
  computeOutput();
  actuatorAttack();
  writeOutput();
}
```

The behavior of the attack is implemented inside the control FMU

Analysis of the attacks with co-simulation

- Co-simulation allows us to analyze the impact of attacks
  - Gaining all the advantages of the co-simulation
    - ✓ (see slides on CPS)

- Exhaustive simulation of the behavior of the system under attack
  - Can be infeasible
  - Initial results can be assumed as general results
  - Results can be misinterpreted

Formal methods can help

- Formal methods provides results with general validity
  - We can consider different experiments at once
    - ✓ FORALL parameters values IT IS TRUE THAT….
    - ✓ FORALL input values IT IS TRUE THAT…
    - ✓ FORALL $t > t_1$ IT IS FALSE THAT…
  - The formal systems prevents users from making mistakes
    - ✓ Discharge the TCCs
    - ✓ Use a well founded logic for reasoning
    - ✓ Rigorous application of the logic reasoning

Drawbacks of formal methods

- Building a formal model of the system under analysis
  - A team of expert users
  - An heterogeneous team
  - Poor graphical results
  - A lot of time

- Proving the formulae
  - Are they actually true?
  - On which subset are they true?
  - Are the hypothesis correct?

Merge co-simulation and Formal methods

- The advantages of one approach are the drawbacks of the other
  - and vice-versa

- Combining the two approaches can provide the best tradeoff between
  - Effort for the analysis
  - Validity of the results

- The combination of the two approaches is still an open field