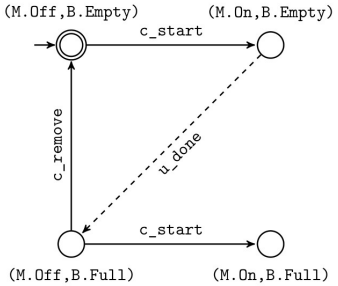
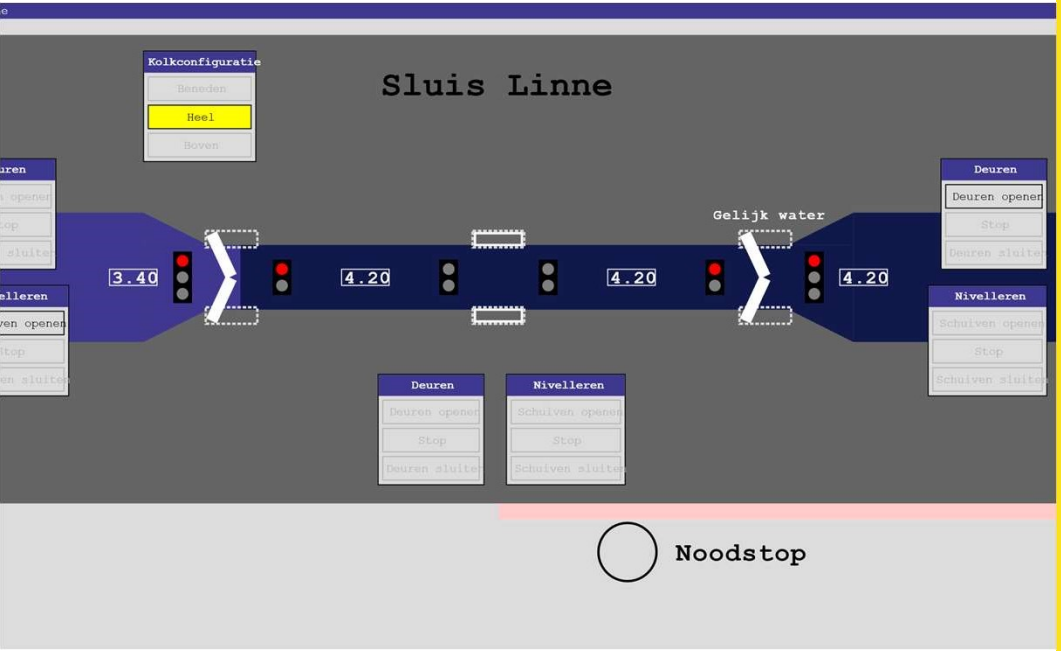


R: requirement c_remove needs M.Off





Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

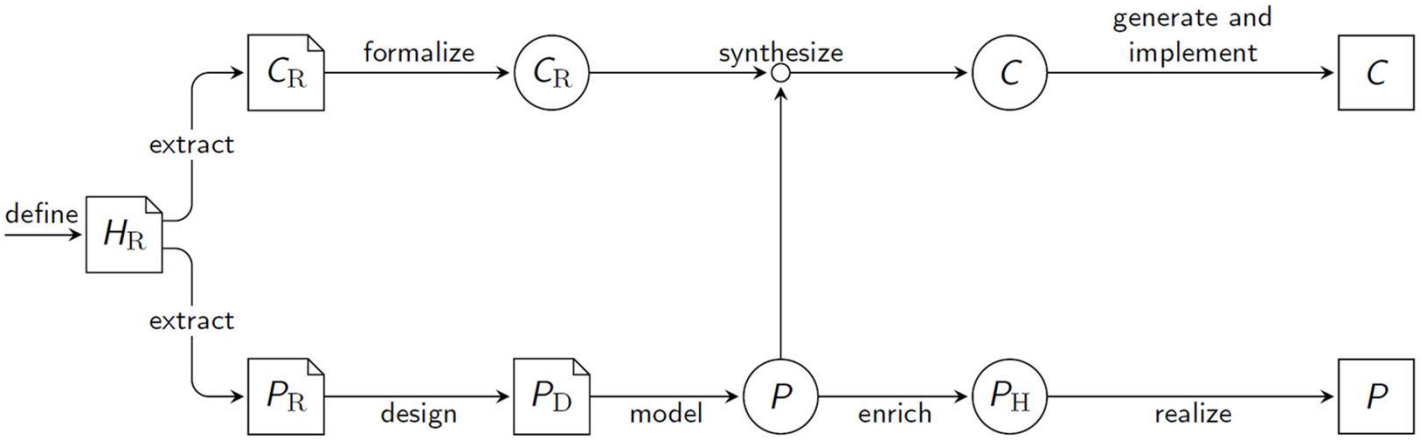
Technische kant SBE

Marktconsultatie

Lars Moormann
Adviseur industriële automatisering GPO

29-05-24

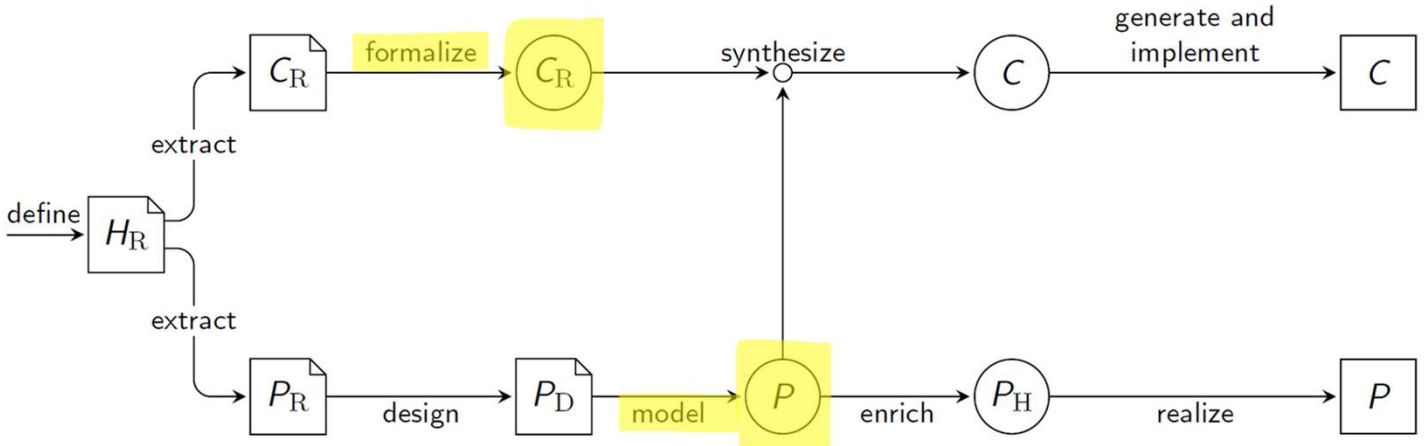
Synthese-gebaseerd ontwerpproces



= document, = model, = realization.

H = high-level, C = controller, S = supervisor, P = plant, R = requirement, D = design, H = hybrid.

Synthese-gebaseerd ontwerpproces



= document, = model, = realization.

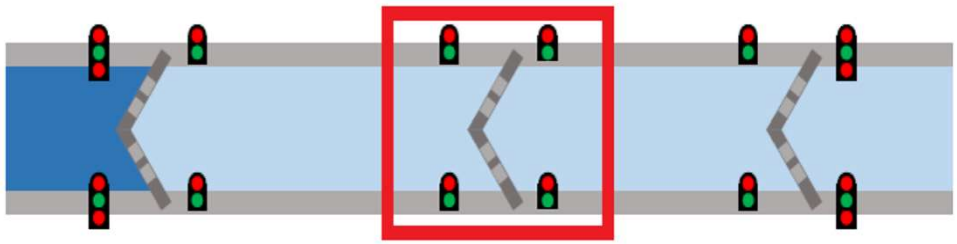
H = high-level, C = controller, S = supervisor, P = plant, R = requirement, D = design, H = hybrid.

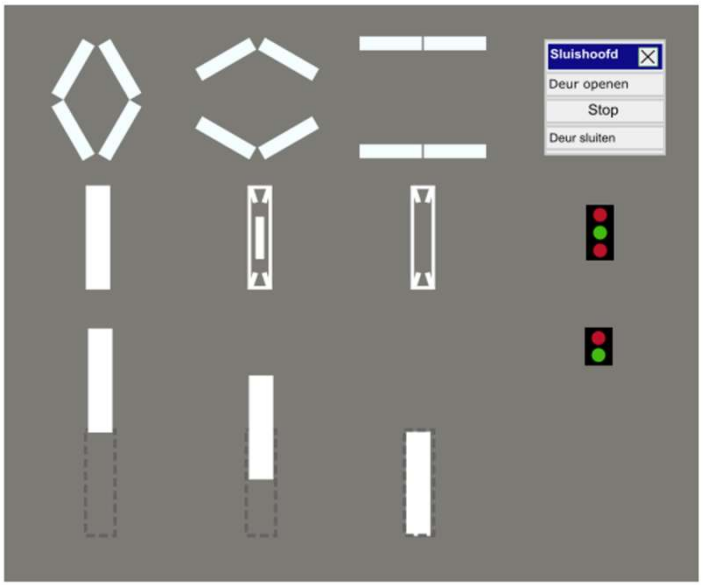
Het gebruik van assemblers

- Doel: sneller SBE simulatiemodellen ontwikkelen
- Aanpak: op basis van een configuratiebestand (voor een sluis of brug) automatisch 90% van het SBE model genereren.
- Sluizenassembler is vorig jaar in een EngD project op de TU/e ontwikkeld (Marzhan Baubekova), en wordt nu beheerd en toegepast binnen RWS.
- Bruggenassembler wordt op dit moment in een EngD project ontwikkeld (Luka Gradinac).

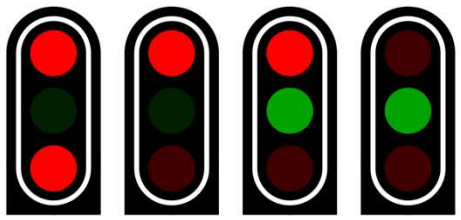
Configuratieparameters sluis

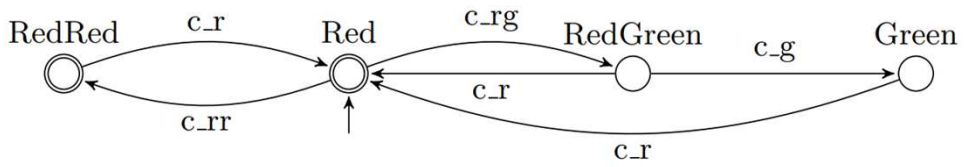
- Een sluis kan geconfigureerd worden in de assembler met, o.a., de volgende parameters:
  - Aantal sluishoofden
  - Waterhoogtes rondom sluis
  - Deurtypen per sluishoofd
  - Nivelleermiddelen per sluishoofd
  - Vaarseintypen per sluishoofd





CIF code voor plant model in ESCET






```
44 // Invaarsein actuator
45 plant def InvaarseinActuator():
46   controllable c_r, c_rg, c_g, c_rr;
47
48   location RedRed:
49     marked;
50     edge c_r goto Red;
51
52   location Red:
53     initial;
54     marked;
55     edge c_rg goto RedGreen;
56     edge c_rr goto RedRed;
57
58   location RedGreen:
59     edge c_g goto Green;
60     edge c_r goto Red;
61
62   location Green:
63     edge c_r goto Red;
64 end
```

CIF code voor eisen model in ESCET

```
group Besturingseisen:
    group Veiligheidsfuncties:
        group VF_I:
            //Indien een nivelleermiddel op het andere sluishoofd niet gesloten is, mag een nivelleermiddel niet geopend worden.
            requirement VF_I_1: not SluisLinne.Bovenhoofd.NivelleermiddelLinks.gesloten disables SluisLinne.Benedenhoofd.NivelleermiddelLinks.Actuator.c_openen;
            requirement VF_I_2: not SluisLinne.Bovenhoofd.NivelleermiddelLinks.gesloten disables SluisLinne.Benedenhoofd.NivelleermiddelRechts.Actuator.c_openen;
            requirement VF_I_3: not SluisLinne.Bovenhoofd.NivelleermiddelRechts.gesloten disables SluisLinne.Benedenhoofd.NivelleermiddelLinks.Actuator.c_openen;
            requirement VF_I_4: not SluisLinne.Bovenhoofd.NivelleermiddelRechts.gesloten disables SluisLinne.Benedenhoofd.NivelleermiddelRechts.Actuator.c_openen;

            requirement VF_I_5: not SluisLinne.Benedenhoofd.NivelleermiddelLinks.gesloten disables SluisLinne.Bovenhoofd.NivelleermiddelLinks.Actuator.c_openen;
            requirement VF_I_6: not SluisLinne.Benedenhoofd.NivelleermiddelLinks.gesloten disables SluisLinne.Bovenhoofd.NivelleermiddelRechts.Actuator.c_openen;
            requirement VF_I_7: not SluisLinne.Benedenhoofd.NivelleermiddelRechts.gesloten disables SluisLinne.Bovenhoofd.NivelleermiddelLinks.Actuator.c_openen;
            requirement VF_I_8: not SluisLinne.Benedenhoofd.NivelleermiddelRechts.gesloten disables SluisLinne.Bovenhoofd.NivelleermiddelRechts.Actuator.c_openen;
        end

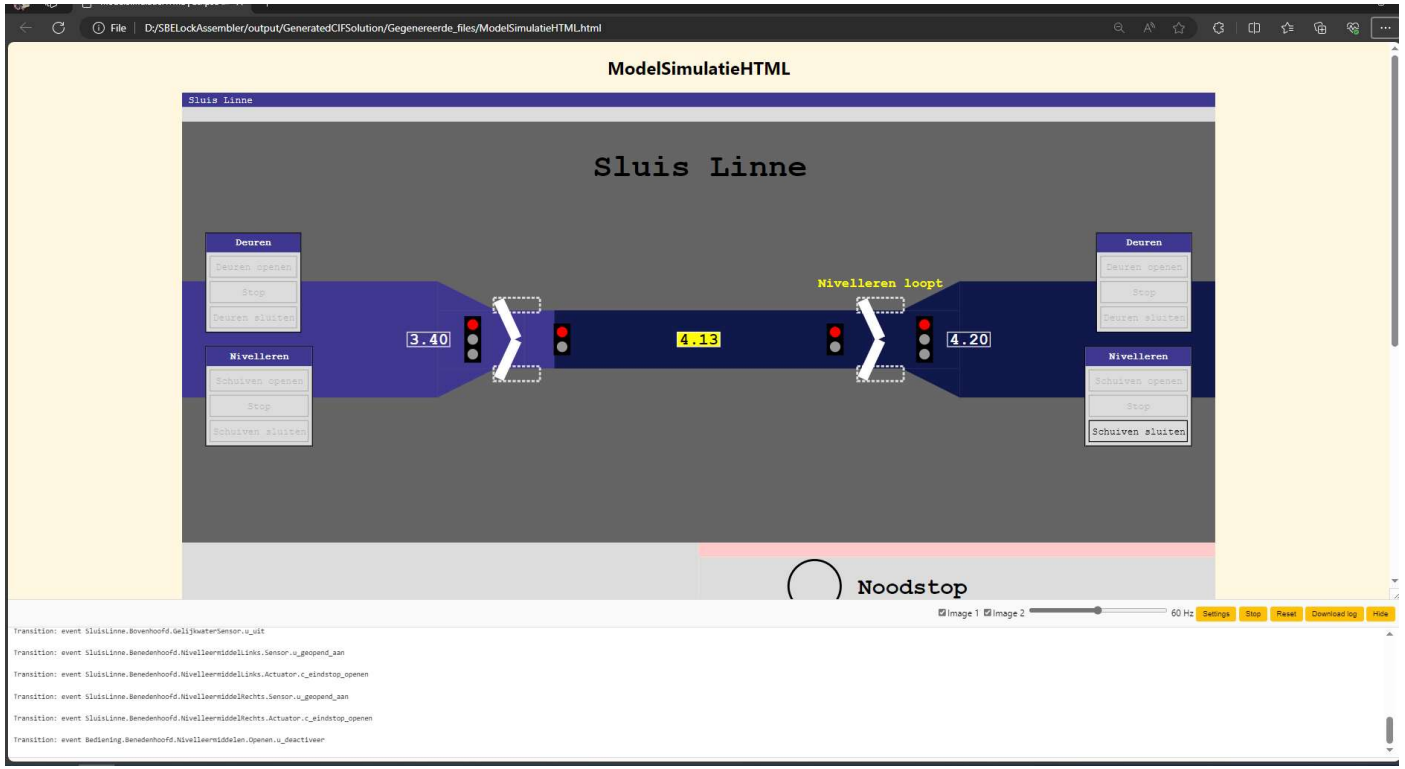
        group VF_II:
            //Indien een deur op het andere sluishoofd niet gesloten is, mag een nivelleermiddel niet geopend worden.
            requirement VF_II_1: not SluisLinne.Bovenhoofd.DeurLinks.gesloten disables SluisLinne.Benedenhoofd.NivelleermiddelLinks.Actuator.c_openen;
            requirement VF_II_2: not SluisLinne.Bovenhoofd.DeurLinks.gesloten disables SluisLinne.Benedenhoofd.NivelleermiddelRechts.Actuator.c_openen;
            requirement VF_II_3: not SluisLinne.Bovenhoofd.DeurRechts.gesloten disables SluisLinne.Benedenhoofd.NivelleermiddelLinks.Actuator.c_openen;
            requirement VF_II_4: not SluisLinne.Bovenhoofd.DeurRechts.gesloten disables SluisLinne.Benedenhoofd.NivelleermiddelRechts.Actuator.c_openen;

            requirement VF_II_5: not SluisLinne.Benedenhoofd.DeurLinks.gesloten disables SluisLinne.Bovenhoofd.NivelleermiddelLinks.Actuator.c_openen;
            requirement VF_II_6: not SluisLinne.Benedenhoofd.DeurLinks.gesloten disables SluisLinne.Bovenhoofd.NivelleermiddelRechts.Actuator.c_openen;
            requirement VF_II_7: not SluisLinne.Benedenhoofd.DeurRechts.gesloten disables SluisLinne.Bovenhoofd.NivelleermiddelLinks.Actuator.c_openen;
            requirement VF_II_8: not SluisLinne.Benedenhoofd.DeurRechts.gesloten disables SluisLinne.Bovenhoofd.NivelleermiddelRechts.Actuator.c_openen;
        end

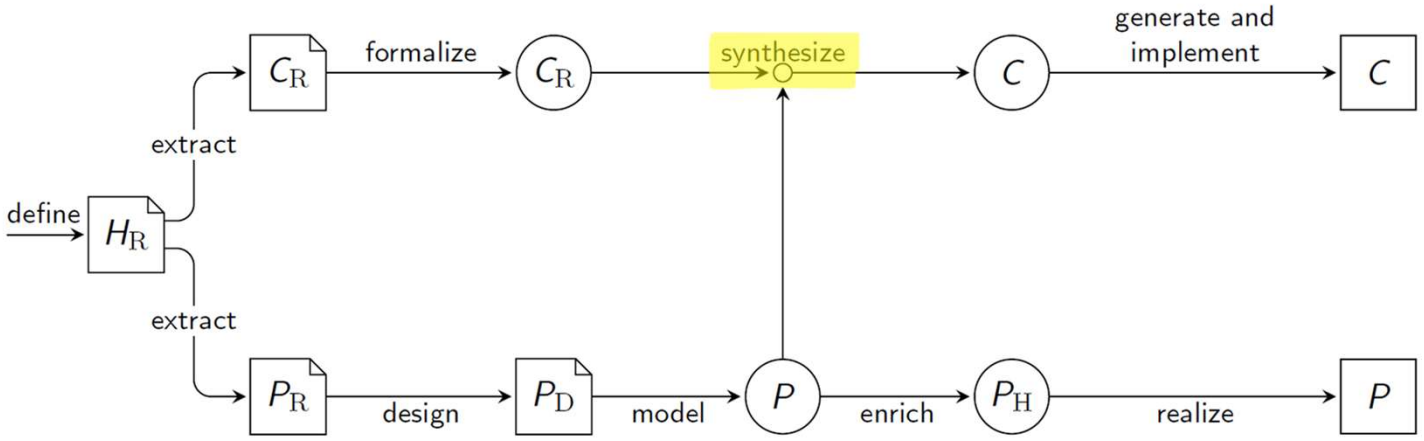
        group VF_III:
            //Indien de gelijkwatersensor bij een deur ongelijk aangeeft, mag de deur niet geopend worden.
            requirement VF_III_9: SluisLinne.Bovenhoofd.GelijkwaterSensor.ongelijk disables SluisLinne.Bovenhoofd.DeurLinks.Actuator.c_openen;
            requirement VF_III_10: SluisLinne.Bovenhoofd.GelijkwaterSensor.ongelijk disables SluisLinne.Bovenhoofd.DeurRechts.Actuator.c_openen;

```

HTML simulatiemodel



Synthese-gebaseerd ontwerpproces



= document, = model, = realization.

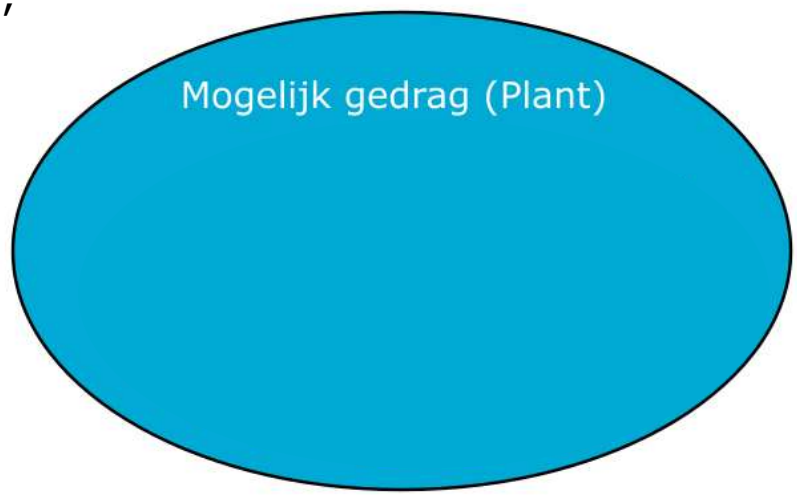
H = high-level, C = controller, S = supervisor, P = plant, R = requirement, D = design, H = hybrid.

Supervisor synthese

- Met het (gegenereerde) plant model en eisen model kan een besturingsmodel (supervisor) gesynthetiseerd worden.
- Deze supervisor:
  - voldoet gegarandeerd aan de ingevoerde eisen,
  - bevat geen deadlock toestanden,
  - blokkeert alleen controleerbaar gedrag,
  - en is maximaal toelaatbaar.

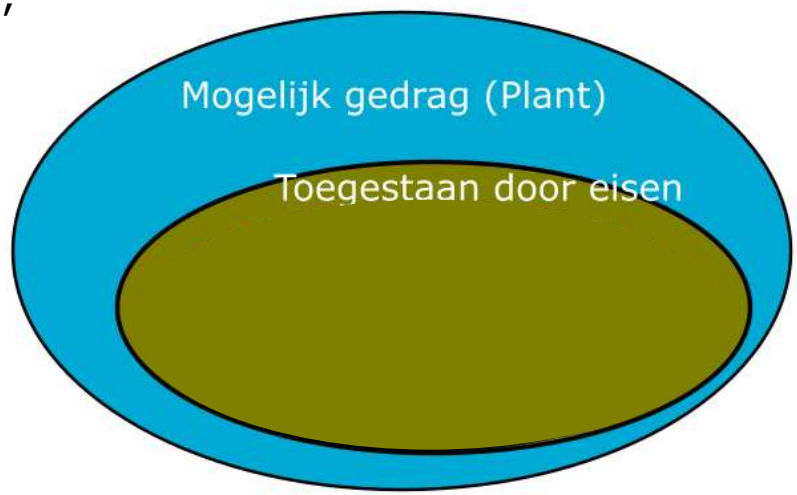
Supervisor synthese

- Met het (gegenereerde) plant model en eisen model kan een besturingsmodel (supervisor) gesynthetiseerd worden.
- Deze supervisor
  - voldoet gegarandeerd aan de ingevoerde eisen,
  - bevat geen deadlock toestanden,
  - blokkeert alleen controleerbaar gedrag,
  - en is maximaal toelaatbaar.



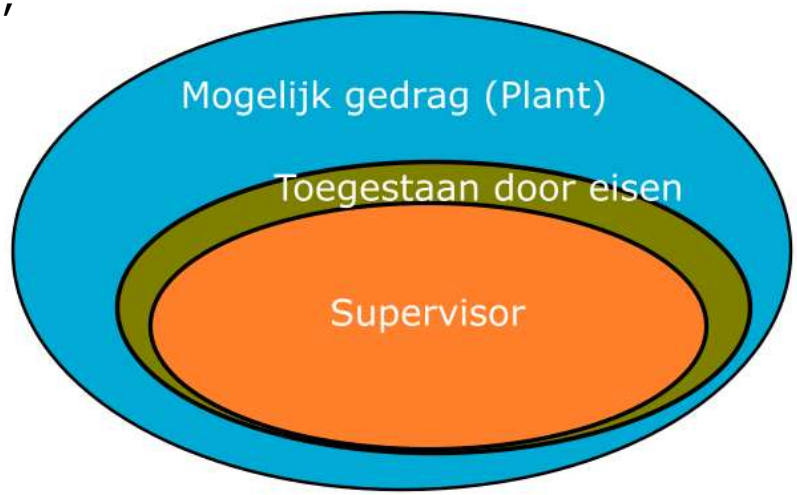
Supervisor synthese

- Met het (gegenereerde) plant model en eisen model kan een besturingsmodel (supervisor) gesynthetiseerd worden.
- Deze supervisor
  - voldoet gegarandeerd aan de ingevoerde eisen,
  - bevat geen deadlock toestanden,
  - blokkeert alleen controleerbaar gedrag,
  - en is maximaal toelaatbaar.



Supervisor synthese

- Met het (gegenereerde) plant model en eisen model kan een besturingsmodel (supervisor) gesynthetiseerd worden.
- Deze supervisor
  - voldoet gegarandeerd aan de ingevoerde eisen,
  - bevat geen deadlock toestanden,
  - blokkeert alleen controleerbaar gedrag,
  - en is maximaal toelaatbaar.

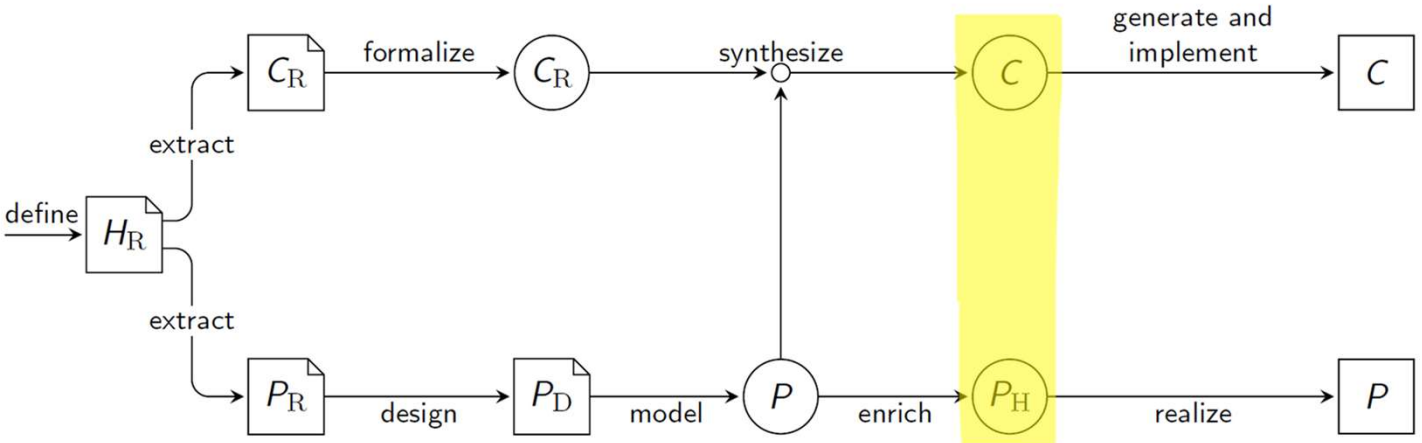


Supervisor synthese

- Met het (gegenereerde) plant model en eisen model kan een besturingsmodel (supervisor) gesynthetiseerd worden.
- Deze supervisor
  - voldoet gegarandeerd aan de ingevoerde eisen,
  - bevat geen deadlock toestanden,
  - blokkeert alleen controleerbaar gedrag,
  - en is maximaal toelaatbaar.



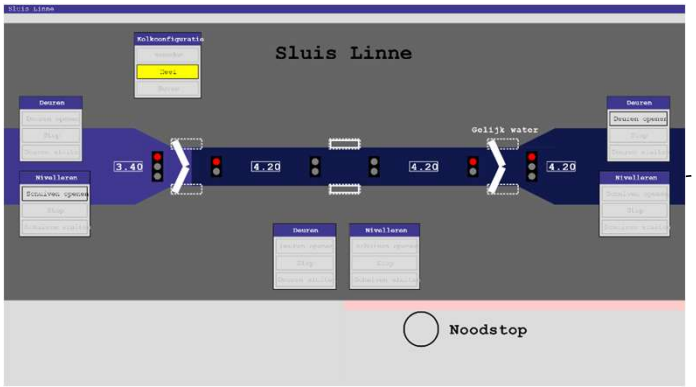
Synthese-gebaseerd ontwerpproces



= document, = model, = realization.

H = high-level, C = controller, S = supervisor, P = plant, R = requirement, D = design, H = hybrid.

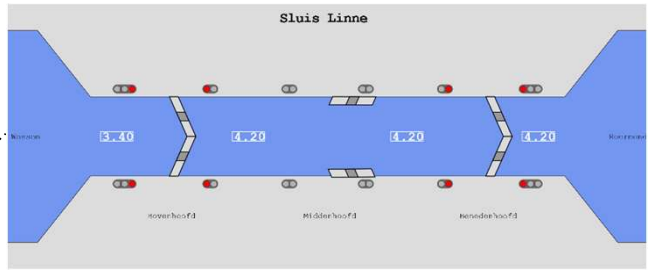
Simulatie



Bedienscherm

Gesynthetiseerde besturing

Virtueel systeem



Verdere mogelijkheden

- Genereren executeerbaar HTML simulatiebestand
- Formele checks t.b.v. PLC implementatie
- Simuleren met I/O signalen
- Genereren PLC code
- Simuleren met geïmplementeerde PLC code (Hardware-in-the-Loop)

Demo van SBE proces met assembler