Engineering based on mathematical models

Ramon Schiffelers

joint work with

Rolf Theunissen, Bert van Beek,
Asia van de Mortel-Fronczak, Koos Rooda

Systems Engineering Group
Dept. of Mechanical Engineering
Eindhoven, University of Technology

Oktober 9, 2008

Background

The work presented is carried out in the Darwin project

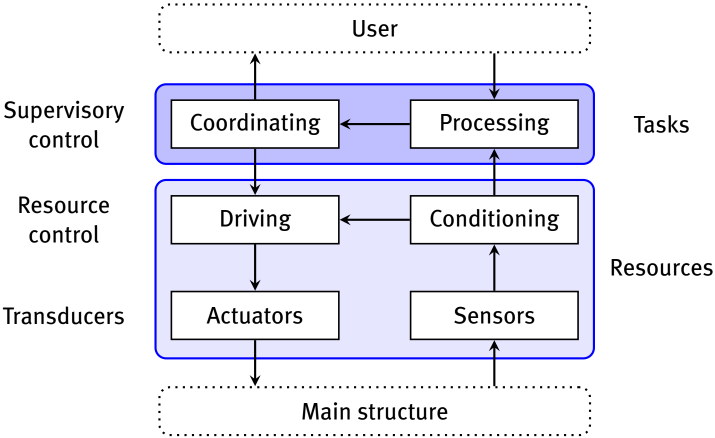
- **Objective**
  Develop architectures, methods and tools for optimizing system evolvability. i.e. the ability of a system to evolve easily in the face of changing requirements.
- **Industrial case**
  MRI scanners: complex systems, about 10^7 lines of code
- **Organization**
  - *Academic partners* Delft University of Technology, Eindhoven University of Technology, University of Groningen (RuG), University of Twente, and the Vrije Universiteit Amsterdam
  - *Industrial partners* Philips Healthcare, Philips Research
  - *Project Management* Embedded Systems Institute (ESI)

See http://www.esi.nl/projects/darwin

Outline

- Supervisory control
- Model-based Engineering (MBE)
- Supervisory Control Synthesis (SCS)
- Supervisory control design
  - conventional
  - using MBE
  - using MBE and SCS
- Industrial case study: Patient support system of a MRI scanner
- Concluding remarks

Supervisory control in high-tech systems



Model-based engineering

Framework

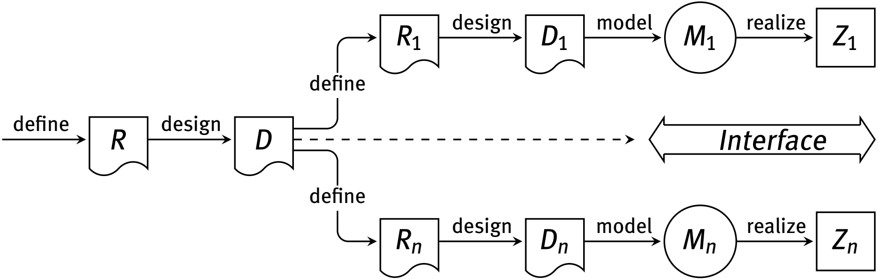
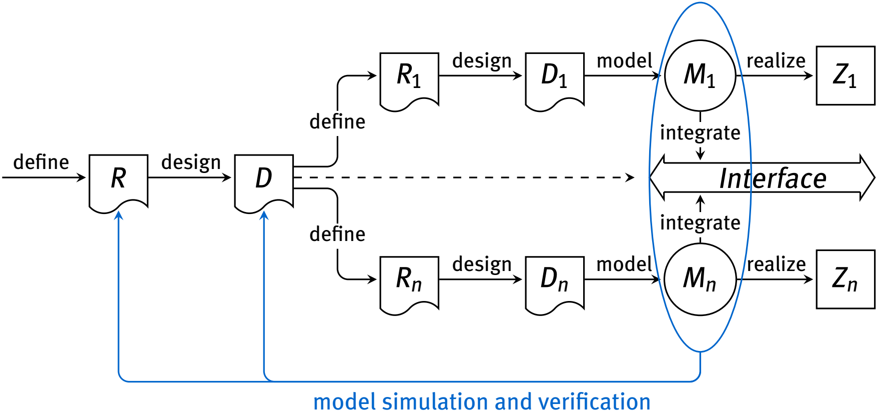


Figure inspired by the TANGRAM project

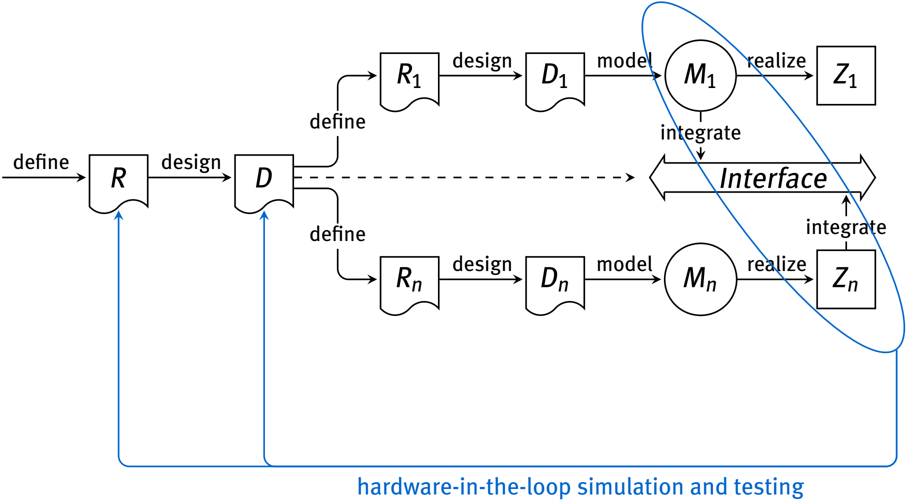
Model-based engineering

Simulation and verification

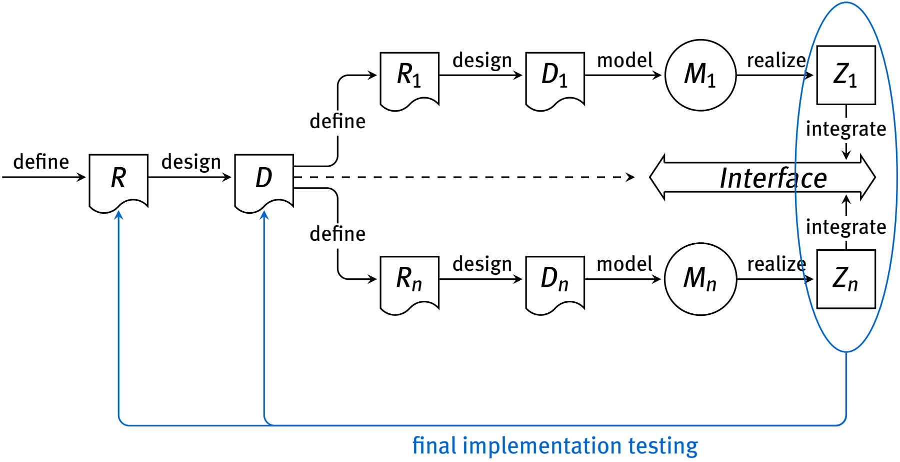


Model-based engineering

Early integration



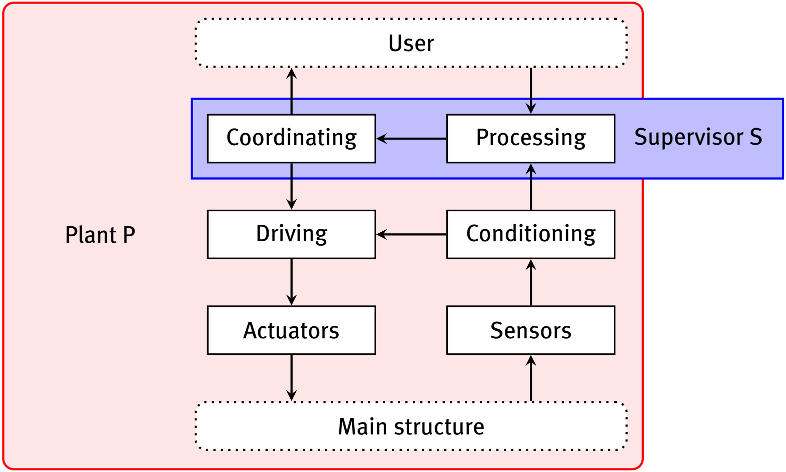
Final implementation testing



Systems view

A system can be divided in

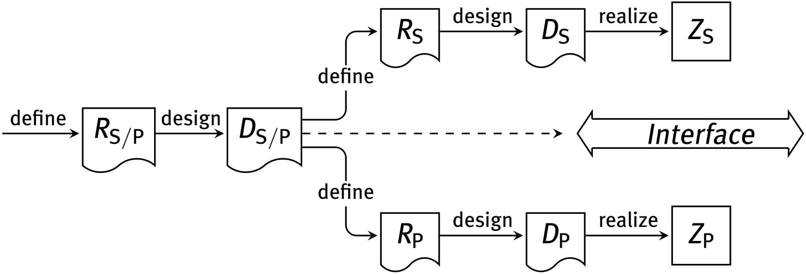
- (uncontrolled) Plant P
- Supervisor (controller) S



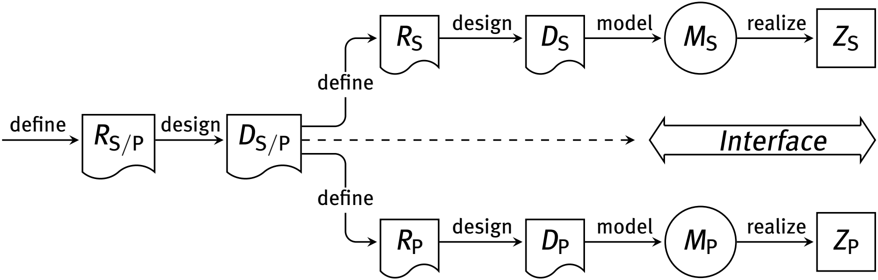
Supervisor S ensures that plant P satisfies its control requirements R_S.

Supervisory control design

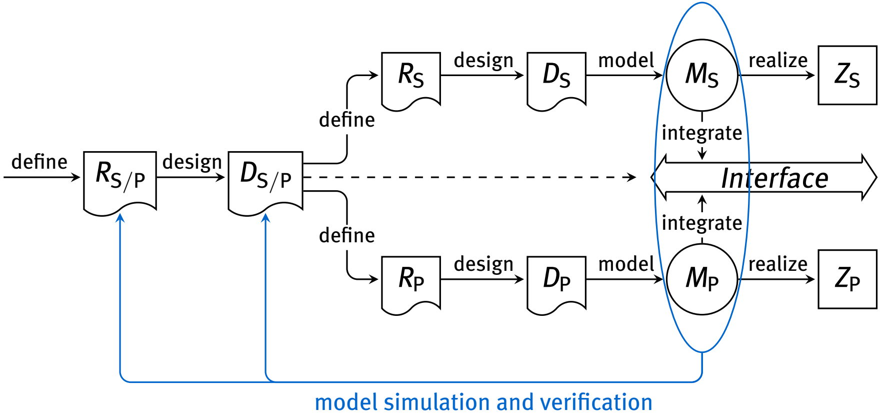
Conventional design



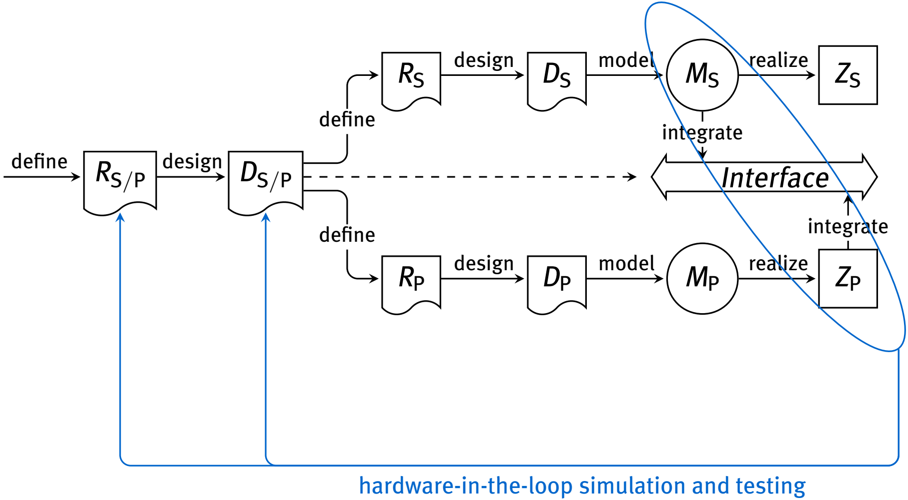
Model-based Engineering



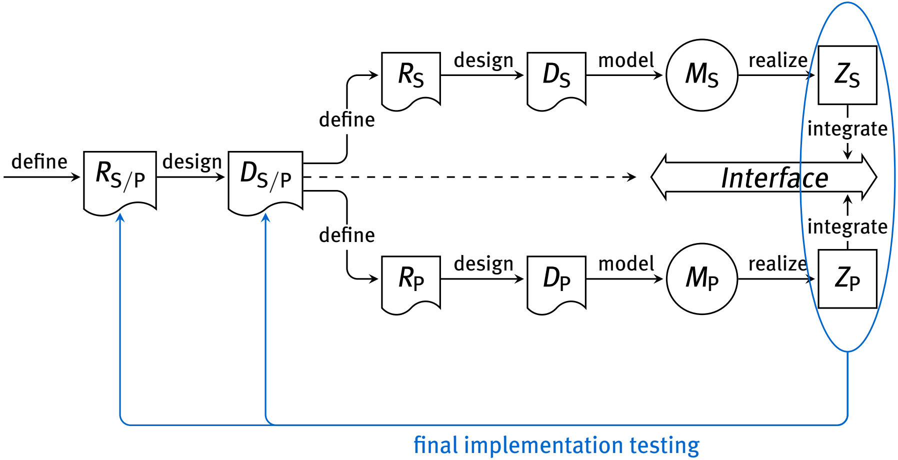
Model-based Engineering



Model-based Engineering



Model-based Engineering



Supervisory Control Synthesis (SCS)

The resulting supervisor is

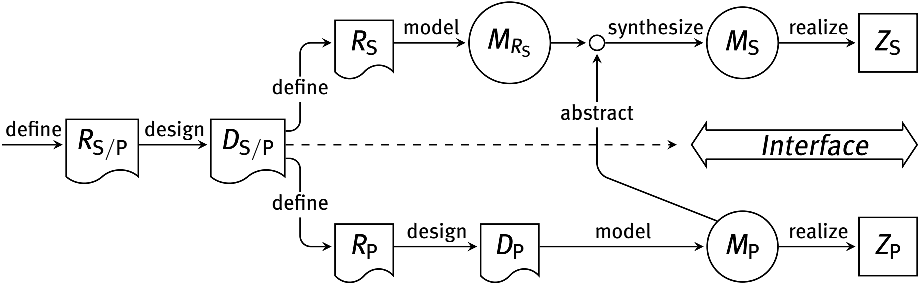
- by construction mathematically correct w.r.t. M_{R_S}
- non-blocking (deadlock and livelock free)
- maximally permissive allowing selection of 'optimal' sequence of events

Approach:

- Model (uncontrolled) plant $\Longrightarrow$ M_P (hybrid model)
- Abstract from M_P (hybrid model) $\Longrightarrow$ M_P (discrete-event model)
- Model control requirements R_S that determine when events may happen $\Longrightarrow$ M_{R_S} (formal requirements)
- Synthesize the supervisor $\Longrightarrow$ M_S (discrete-event model)

Supervisory control design

Model-based Engineering and Supervisory Control Synthesis

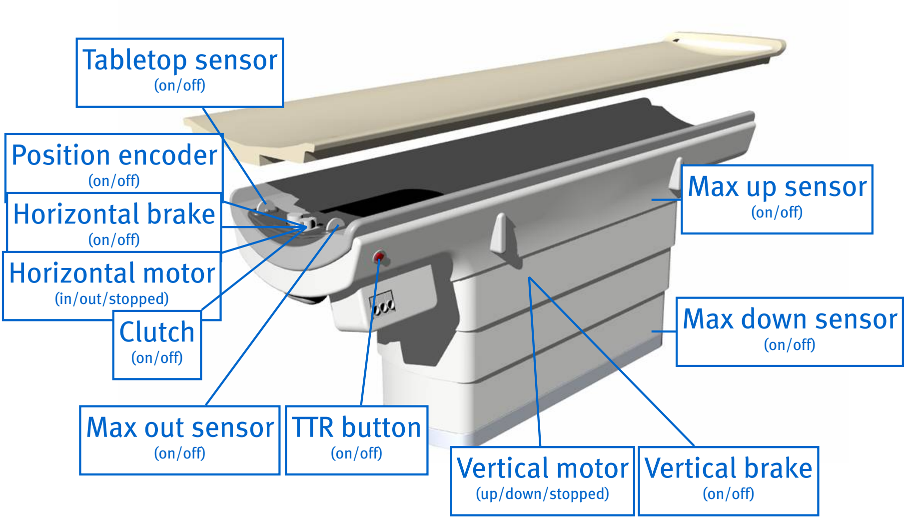


Industrial case study

Patient support system

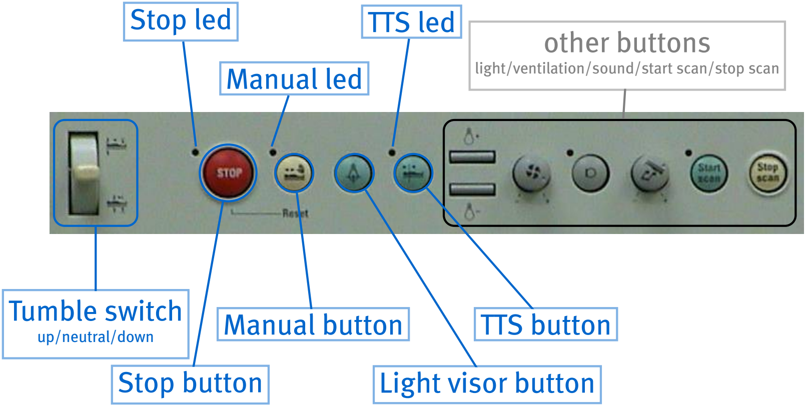
Patient support system

Table



Patient support system

PICU (user interface)



Uncontrolled plant M_P

Uncontrolled plant M_P consists of 17 small automata describing:

- Horizontal axis
- Vertical axis
- User interface buttons

In total 1296 states and 27360 transitions for the uncontrolled plant.

Patient support system

Control requirements M_{R_S}

- The model of the control requirements M_{R_S} consists of 16 small automata
- Examples of requirements:
  - Do not move beyond end sensors
  - Only motorized movement if clutch is active
  - No motorized movement if Table-Top-Release active
  - Only move vertically if horizontally in maximal out position
  - Tumble switch moves table up and down, or in and out
  - ...

Patient support system

Supervisor synthesis

- The model of the supervisor M_S consists of 2816 states and 21672 transitions
- Supervisor synthesis takes a minute on a desktop pc

- The synthesized supervisor has been simulated in parallel with the (hybrid) model of the plant
- The synthesized supervisor has been simulated in real-time with the actual patient support system (hardware-in-the-loop simulation)

Concluding remarks

- Eliminated manual design of the supervisor
- Combination of MBE and SCS works very well, also on a complex industrial case
- Lots of theory available for supervisory control synthesis
  - monolitic / modular / decentralized / hierarchical / interface-based supervisors
  - supervision under partial observation
  - event-based / state-based supervision
  - different formalisms for plant modeling and requirement specifications

Concluding remarks

Q-T-C triangle

- *Quality*: $Q \uparrow$
  The synthesized supervisor is by construction mathematically correct w.r.t. the modeled requirements
- *Time-to-market*: $T \downarrow$
  A change in required functionality leads to re-modeling of the requirements only
- *Costs*: $C \approx$
  The costs remain more or less the same

Engineering based on mathematical models

Ramon Schiffelers

joint work with

Rolf Theunissen, Bert van Beek,
Asia van de Mortel-Fronczak, Koos Rooda

Systems Engineering Group
Dept. of Mechanical Engineering
Eindhoven, University of Technology

Oktober 9, 2008