Supervisory Control of Manufacturing Machines

Industrial applications

J.M. van de Mortel-Fronczak in cooperation with

J.E. Rooda

October 15, 2013
Outline

- Introduction
- Supervisory control synthesis
- Tools
- Industrial cases
- Projects
Embedded systems
Trends in embedded systems development

Expressed in terms of key performance indicators \((F, Q, T, C)\):

- Functionality \(F\) and complexity increase
- Product quality \(Q\) should not decrease
- More and complex control software code
- Testing control software time-consuming
- Time-to-market \(T\) and product cost \(C\) increase
Traditional systems engineering
Synthesis-based systems engineering
Supervisory control problem

Plant $P$ and supervisor $S$ form a discrete-event system (DES):

- $P$ under control of $S$ ($S/P$) satisfies requirement $R$
- $S$ does not disable uncontrollable events
- Output of $S$ only depends on observable outputs of $P$
- $S/P$ is nonblocking
- $S$ is optimal (maximally permissive)
Supervisory control theory

- Provides means to synthesize $S$
- Conceptually simple framework (based on DES)
- Computational complexity is high for systems of industrial size

Several advanced techniques to reduce synthesis complexity:

- Modular and extended modular
- Coordinated modular
- Hierarchical
- Interface-based hierarchical
- Coordinated distributed
- Aggregated distributed
Tool chain for SCS

- Algorithms for synthesis
- Model transformations
- Common Interchange Format
Synthesis tools

- TCT — University of Toronto
- Supremica — Chalmers University of Technology
- DESTool — University of Erlangen-Nuremberg
- DESUMA — University of Michigan
- SuSyNA — Eindhoven University of Technology
Industrial cases

Supervisory control synthesis for:

- Patient support system of an MRI scanner
- Coordination of maintenance procedures in printers
- Theme park vehicles
Patient support system of an MRI scanner

Safe tabletop handling

- User interface
- Light sight
- Bore
- Patient support table
Control requirements

- Ensure that the tabletop does not move beyond its vertical and horizontal end positions.

- Prevent collisions of the tabletop with the magnet.

- Define the conditions for manual and automatic movements of the tabletop.

- Enable the operator to control the system by means of the manual button and the tumble switch.
Results

- A centralized supervisor was synthesized using the TCT tool.
- The system under control of the supervisor was validated using simulation.
- The supervisor was tested on the real system.
- After a functional change, approximately four hours work was needed to repeat the above steps.
Results

- Plant model: 672 states.
- Requirement model: 4.128 states.
- The supervisor: 2.976 states.
Coordination of maintenance procedures in printers
Control requirements

- Maintenance operations may only be performed if the power mode of the printing process is Standby.

- Maintenance operations should be scheduled if their soft deadline is reached and no print jobs are in progress or if their hard deadline is reached.

- Only scheduled maintenance operations can be started.

- The power mode of the printing process should conform to the mode determined by the print job managers unless it is overridden by a pending maintenance operation.
Results

- A centralized supervisor was synthesized using the synthesis tool based on state-tree structures.

- The system under control of the supervisor was validated using simulation.

- The supervisor is converted to C++ for execution on the existing control platform.
Results

- Plant model: 25 automata with 2 to 24 states.
- Requirements: 23 generalized state-based expressions (more than 500 standard state-based expressions).
- The supervisor: $6 \cdot 10^6$ states.
Theme park vehicle

Handling of proximity, emergency, and hardware errors in theme park vehicles

- Scene Program Handler (on/off)
- Steer Motor (on/off)
- Ride Control (start/stop)
- Battery (empty/OK)
- 4 Proximity Sensors (on/off)
- User Interface (3 LEDs/3 buttons) (on/off)
- Drive Motor (on/off/stopped)
- Bumper Switch (on/off)
Control requirements

- To avoid collisions with other vehicles or obstacles, the multimover should drive at a safe speed and stop if the obstacle is too close to it.

- The vehicle should stop immediately and should be powered off when:
  - a collision or a system failure occurs,
  - the battery level is too low.

After the problem is resolved, the multimover should be manually deployed back into the ride by an operator.
**Plant components**

- 17 automata
- 2–4 states per automaton

**LED:**

\[\text{LED}_\text{Off} \xrightarrow{\text{led}_\text{go}_\text{on}} \text{LED}_\text{On} \]

\[\text{led}_\text{go}_\text{off}\]

**Bumper switch:**

\[\text{BS}_\text{Released} \xrightarrow{\text{bs}_\text{press}} \text{BS}_\text{Pressed} \]

\[\text{bs}_\text{release}\]
Control requirements

- 30 automata
- 2–7 states per automaton

Reset requirement:

A reset may happen only if the bumper switch is released.
Coordinated distributed event-based synthesis

Modules:

- LED actuation
- Motor actuation
- Button handling
- Emergency handling
- Proximity handling
## Results

Coordinated distributed approach:

<table>
<thead>
<tr>
<th>Module supervisors</th>
<th># states</th>
<th># trans.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED actuation</td>
<td>25</td>
<td>77</td>
</tr>
<tr>
<td>Motor actuation</td>
<td>41</td>
<td>222</td>
</tr>
<tr>
<td>Button handling</td>
<td>193</td>
<td>1541</td>
</tr>
<tr>
<td>Emergency handling</td>
<td>181</td>
<td>2149</td>
</tr>
<tr>
<td>Proximity handling</td>
<td>481</td>
<td>4513</td>
</tr>
</tbody>
</table>

Module supervisors are nonconflicting — no coordination is needed.
Results

- A centralized supervisor was synthesized using the synthesis tool based on state-tree structures.

- A distributed supervisor was synthesized using the synthesis tool based on automaton abstraction.

- The system under control of both supervisors was validated using simulation.

- Both supervisors were tested on the real system.

- After a functional change, approximately four hours work was needed to repeat the above steps.
Conclusions

• Model-based systems engineering contributes to faster product development.

• Supervisor synthesis eliminates manual design of control software and reduces testing effort.

• Successful proofs of concept delivered for implementation of advanced synthesis techniques.

• Event-based distributed framework supports reconfigurability.

• Synthesis-based systems engineering is applicable in industry for developing supervisory controllers.

• Formal models and methods are essential for high-tech systems design.
Recent final projects SE group

Michel Reniers:

- Scalability of Supervisory Control Theory (ASML)
- Validation and verification of a pipeless plant using UPPAAL and SpaceEx
Recent final projects SE group

Bert van Beek:

- Formal modeling of paper path exception handling using the CIF (Océ)
- Supervisory control and real-time implementation of MRI subsystems (Philips Healthcare)
- Evaluation of CIF and development of CIF to ST model transformations for real-time control
- Supervisory control and real-time implementation of the Veghel Airport Bagage handling system (VanderLande Industries)
Recent final projects SE group

Asia van de Mortel:

- Application of supervisor synthesis to the design of cruise control (DAF)
- Optimization of sheet printing control software (Océ)
- Supervisory control of electron microscopes (FEI)
Possible internship destinations

- Chalmers University of Technology, Sweden
- Technische Universität Dortmund, Germany
- Nanyang Technological University, Singapore
- University of Jinan, China
- McMaster University, Hamilton, Canada
- ASML, Veldhoven, The Netherlands