30 years of the Ramadge-Wonham Theory of Supervisory Control: A Retrospective and Future Perspectives

S. Lafortune, K. Rudie, and S. Tripakis

U. Michigan, Queen’s U., Aalto U.

CDC 2017 Workshop
Melbourne, Australia

11 December 2017
Outline

SCT @ 30

SCT, Reactive Synthesis, and Formal Methods in Control

Decentralized Control and Undecidability

Workshop Schedule
The Beginnings

The two SICOPT papers of Ramadge & Wonham published in 1987 [9, 15]
The Context

- Discrete Event Systems
  - discrete state space
  - event-driven dynamics

- Regular languages and their finite-state automata representations
  - Events: Controllable or not; Observable or not
  - Strings of events

- The Feedback Loop
Regular language specifications

System: An automaton \((G)\)

Specification: Another automaton \((H)\)

**Safety:** WLOG: no illegal states reached. Requires suitable state-space refinement of \(G\) using \(H\)

**Non-blockingness:** no deadlocks or livelocks w.r.t. marked states (double circles)
Comments on Supervisor:

▶ The system has its uncontrolled behavior (there is a “plant”)

▶ The supervisor disables events to restrict the system behavior; i.e., the supervisor enables a set of events

▶ We want the supervisor to be maximally permissive
  ▶ Optimality criterion is set inclusion
  ▶ Only disable an event if absolutely necessary to guarantee safety and non-blockingness
Comprehensive Theory

- Discrete-event system-theoretic properties for *necessary and sufficient* conditions for *existence* of solution
  - controllability (about *actuators*)
  - observability, coobservability (about *sensors* and *actuators*)
  - non-conflictingness

- Effective computational algorithms for *supervisors*
  - Fix-point characterizations on languages: finitely-convergent iterative algorithms on automata

- Variety of control architectures:
  - decentralized-information
  - distributed: horizontal or vertical modularity
Recent Applications of SCT

- Automated manufacturing [7]
- Transportation [4]
- Patient support systems [12]
- Process control [10]
- Web Services Composition [1]

Sources: houstonchronicle.com; [12]; [4]
DES Supervisory Control problems are everywhere now!

*Higher-level control logic* in Network Control Systems and Cyber-Physical Systems

Challenges: *Modeling / Abstraction / Specification* and Scalability of Synthesis
Outline

SCT @ 30

SCT, Reactive Synthesis, and Formal Methods in Control

Decentralized Control and Undecidability

Workshop Schedule
Formal Methods in Control

- Modeling: Automata – Petri Nets – Labeled Transition Systems
- Specifications: Regular Languages – GMEC: Generalized Mutual-Exclusion – Temporal Logic
  CTL*, CTL, LTL, co-safe LTL, GR(1), LTLf, etc.
Controller, Plants and Closed-Loop Systems in the Reactive Synthesis Framework

- Reactive Synthesis Problem [8] does not have an explicit plant
  - “Assume-guarantee” approach
    $\phi_{plant} \Rightarrow \phi_{spec}$ (“plant” or “environment”)

- RSCP: reactive synthesis control problem with plants; e.g., Kupferman, Madhusudan, et al.: [5, 6]:
  plant modeled as (labeled) transition system with system states and environment states (allows to separate controllable and uncontrollable events)

- Formal methods in control: plant modeled as (labeled) transition system, which is then composed with (Rabin, Büchi) automaton translation of temporal logic formula; cf., Belta et al.: [2]
Other Differences

- Supervisors are *parents* – controllers are ... controllers

- Supervisory control asks for *maximally-permissive* behavior – these generally do not exist in reactive synthesis.

- (Most of) supervisory control theory done in a *finite-string* setting – reactive synthesis is about infinite strings

- Specs as Automata (think illegal states) or in Temporal Logic
  - Safety (invariance): easy to map
  - Non-blockingness (reachability) in supervisory control cannot be expressed in LTL but requires CTL:

\[
\phi_{nb} := AG \ EF \ acc
\]
Outline

SCT @ 30

SCT, Reactive Synthesis, and Formal Methods in Control

Decentralized Control and Undecidability

Workshop Schedule
Decentralized Supervisory Control

Each supervisor is a partial-observation supervisor, with its own set of controllable and observable events. Locally controllable and/or observable events may overlap, i.e., $E_{o,i} \cap E_{o,j} \neq \emptyset$ in general.
Decentralized Supervisory Control

<table>
<thead>
<tr>
<th></th>
<th>Arbitrary</th>
<th>Max</th>
<th>NB</th>
<th>NB+Max</th>
</tr>
</thead>
</table>

[3] [Cieslak et al., TAC, 1988]
[11] [Rudie and Wonham, TAC, 1992]
[13] [Thistle, SCL, 2005]
[14] [Tripakis, IPL, 2004]

Table: Decentralized Supervisory Control under Partial Observation

Can we solve the open problems? *(Talk to Rüdiger Ehlers!)*
Outline

SCT @ 30

SCT, Reactive Synthesis, and Formal Methods in Control

Decentralized Control and Undecidability

Workshop Schedule
Workshop Schedule: AM

- 8:30-8:45am: Participants arrive
- 8:45-9:00am: Opening remarks (organizers)
- 9:00-9:30am: Peter Ramadge
- 9:30-10:00am: Martin Fabian
- 10:00-10:30am: Alessandro Giua
- 10:30-10:50am: Morning coffee break
- 10:50-11:20am: Richard Murray
- 11:20-11:50am: Kai Cai
- 11:50-12:00pm: Murray Wonham [presented by Kai Cai]
- 12:00-1:30pm: Lunch (not provided - nearby restaurants)
Workshop Schedule: PM

- 1:30-2:00pm: José Cury
- 2:00-2:30pm: Sanjit Seshia
- 2:30-3:00: Afternoon coffee break
- 3:00-3:30pm: Calin Belta
- 3:30-4:00pm: Hervé Marchand
- 4:00-4:30pm: George Pappas
- 4:30-5:00pm: Necmiye Ozay
- 5:00-5:30pm: Open discussion (all speakers and participants)
References

Automated service composition via supervisory control theory.

*Formal Methods for Discrete-Time Dynamical Systems*.

Supervisory control of discrete-event processes with partial observations.

Application of supervisory control theory to theme park vehicles.

Open systems in reactive environments: Control and synthesis.

*Control and Synthesis of Open Reactive Systems*.

Applied supervisory control for a flexible manufacturing system.

On the synthesis of a reactive module.

Supervisory control of a class of discrete event processes.


