Dealing with uncertainty in safety-critical cyber-physical systems

A control engineering perspective

dr. ir. Sofie Haesaert

Assistant Professor
TU Eindhoven

November 27, 2019
Control engineering — classically

Provide stability, performance and robustness via feedback withstanding physical uncertainty and stochasticity

Mechanical ~1788
Governor & throttle valve
1st automatic control

Analogue
PID control

Digital control
Optimal control
Robust control
Complex systems
Examples of digitally controlled systems

Models for digital control

\[
\begin{align*}
\text{state: } & x(t + 1) = F(x(t), u(t)) + \text{disturbances} \\
\text{output: } & y(t) = H(x(t), u(t)) + \text{sensor noise}
\end{align*}
\]

Dynamical systems modeled via ordinary differential equation

\[
\begin{align*}
\text{state: } & \dot{x}(t) = f(x(t), u(t)) + \text{disturbances} \\
\text{output: } & y(t) = h(x(t), u(t)) + \text{sensor noise}
\end{align*}
\]
Control engineering — emerging

Technological innovations lead to increased functionality, complexity and autonomy

Waymo’s fully autonomous driving

Credit: waymo.com
Cyber-physical systems (CPS)

Complex merging of computation into the physical world

Increase of connectivity, functionality, complexity, and autonomy

Physical systems with software for communications, interactions, sensing, and control.

Delivery drones (amazon)

Credit: dryve.com

Autonomous driving

Credit: Amber

Smart grid

Credit: unsplash

Long-term autonomy on Mars rover missions

Credit: NASA/JPL-Caltech
Safety-critical cyber-physical systems

Complex merging of computation into the physical world

Increase of connectivity, functionality, complexity, and autonomy

Physical systems with software for communications, interactions, sensing, and control.

Verify software + physical system

- Uncertain, continuous space models
- Noisy output measurements
- Stochastic disturbances

Software bugs directly affect physical world
Dealing with stochasticity in CPS

How to design and verify digital control?

High-level specifications
- Avoid A until K and eventually visit L …

Physical model
- Wind & temperature
- Component failure
- Human behavior
Dealing with stochasticity in CPS

How to design and verify digital control?

High-level specifications
- e.g., Avoid A until K and eventually visit L …

Physical model
- Wind & temperature
- Component failure
- Human behavior
Dealing with partial & noisy observations

Potential hazard
Potential sample
Rover
Environment

Mission specification
\[ \psi := \neg \text{fail} \cup \text{sample} \]

Partially observable MDP
\[
\begin{align*}
    x_{t+1} &\sim T(\cdot|x_t, u_t) \quad \text{state} \\
    z_t &\sim R(\cdot|x_t, u_t) \quad \text{observations}
\end{align*}
\]

Belief MDP
\[
\begin{align*}
    b_t &= \mathbb{P}(dx_t \mid (u_k, y_k)_{k \leq t}) \quad \text{state} \\
    b_{k+1} &\sim T_b(\cdot|b_k, u_k) \quad \text{belief transitions}
\end{align*}
\]

Abstract problem
Finite MDP \( \tilde{M} \) + specification \( \psi \)
Dealing with partial & noisy observations
How to design and verify digital control?

Control refinement to gMDP
- Preserves guarantees

Computations on abstract model
- Value iterations
- Robust temporal logic satisfaction
Dealing with model uncertainty in CPS

How to verify functionality using data?

Partially unknown system

\[ x_{t+1} = f(x_t, u_t; \theta) + v_t \]
\[ y_t = h(x_t; \theta) + e_t \]

\( \theta = \text{unknown parameter} \)

Solution: Use prior knowledge and data

Compute confidence with Bayesian inference

\[ P \{ M(\theta) \models \psi \mid (u, y)_t \} \]

Data obtained from system

Parameterized model

Sofie Haesaert — Safety-critical cyber-physical systems

S. Haesaert et al. ACC15, CDC15, Automatica17
Dealing with model uncertainty in CPS

How to collect the right data efficiently?

Design experiment input to gain information on property satisfaction.

\[ P(\mathbf{M}(\theta) \models \psi \mid \{u, y\}_t) \]

= Optimal control problem

Maximize probability of reaching decision

\[ P(\mathbf{M}(\theta) \models \psi \mid \{u, y\}_t) \geq 1 - \delta = \text{accept} \]

\[ P(\mathbf{M}(\theta) \models \psi \mid \{u, y\}_t) \leq \delta = \text{reject} \]

Some data is expensive.

Sofie Haesaert — Safety-critical cyber-physical systems

S. Haesaert et al. ACC15, ECC16
Dealing with uncertainty in safety-critical cyber-physical systems
A control engineering perspective

dr. ir. Sofie Haesaert
Assistant Professor
TU Eindhoven
The Netherlands

Contact me at
Sofiehaesaert.com
s.haesaert@tue.nl

Thank you for your attention