Formal Analysis of Timing Effects on Closed-loop Properties of Cyber Physical Systems

Arne Hamann, Corporate Research, Robert Bosch GmbH

Joint work with: Matthias Wöhrle (Bosch), Goran Frehse (Université Joseph Fourier Grenoble), Sophie Quinton (INRIA Grenoble)
Outline

- Problem statement & goals
- Interaction model for co-engineering between control and real-time engineering
- Electro Mechanic Braking System (EMB)
- Formal analysis of EMB system using hybrid automaton and reachability analysis
- Conclusion
Formal Analysis of Timing Effects in CPS

System as seen by the control engineer

Sophisticated Control Algorithm

No/Constant Control Delay
Calculation takes 0/constant time

Periodic Sampling, No Jitter

No Output Jitter, “Freshest” value always available

\[ x = Ax + Bu \]
\[ y = C^T x \]

A/D Converter

u_k

D/A Converter

yk

u(t)

y(t)

Write Data

Read Data

3
Formal Analysis of Timing Effects in CPS

System as seen by the real-time engineer

Deadline = Period
WCET, WCRT

\[ \sum_{i=1}^{n} \frac{C_i}{T_i} \leq n \cdot \left( \sqrt{2} - 1 \right) \ln 2 \approx 69.3\% \]

\[ R_i = C_i + \sum_{j \in hp(i)} C_j \left\lfloor \frac{R_i}{T_j} \right\rfloor \leq D_i = T_i \]
## Formal Analysis of Timing Effects in CPS

### Problem Statement - Shortcomings

<table>
<thead>
<tr>
<th>Control engineering</th>
<th>Real-time system engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Theory:</strong></td>
<td><strong>Theory:</strong></td>
</tr>
<tr>
<td>• Equidistant sampling</td>
<td>• Timing models and requirements that are motivated by the runtime system rather than functionality (e.g. deadline = period)</td>
</tr>
<tr>
<td>• Zero input-output latencies</td>
<td><strong>Reality:</strong></td>
</tr>
<tr>
<td><strong>Reality:</strong></td>
<td>• Timing requirements do not exist per se and must be derived from functional requirements</td>
</tr>
<tr>
<td>• Varying execution and response times due to preemption, blocking, data-dependencies, ...</td>
<td><strong>Reality:</strong></td>
</tr>
<tr>
<td>• Sampling interval jitter</td>
<td>• Sampling interval jitter</td>
</tr>
<tr>
<td>• Non negligible response times</td>
<td><strong>Result:</strong></td>
</tr>
<tr>
<td></td>
<td>• Functional integration effects due to timing are unpredictable</td>
</tr>
<tr>
<td></td>
<td>• Severe migration problems in case of platform modifications</td>
</tr>
</tbody>
</table>
Formal Analysis of Timing Effects in CPS

Goals

- **Co-engineering** between real-time and control engineering

- Assessment of functional behavior under the influence of resource sharing **during design time on PC**

- Systematically **derive timing requirements** that are necessary to fulfill functional requirements

- Use these timing requirements for **system synthesis** using adequate platform mechanisms
Formal Analysis of Timing Effects in CPS

Current Interaction Model

Plant, Control Problem, Functional requirements

Control Engineering (per control problem)

- Analysis of plant dynamics (e.g. time constants)
- Specification of problem class
- Choice/derivation of control algorithm
- Discretization of control laws

Hardware Architecture, Tool Chain

Real-time Engineering

- Equations / Code
  - Desired sampling rate (range)
- Integration of n control functions
- Mapping to cores
- Selection of scheduling strategy
- Assignment of scheduling parameters (offsets, priorities, ...)
- Assignment of execution orders and sequences

Problems:
- OK only means sampling rate met
- NOT that the functionality works
- Oversampling to compensate unknown integration effects

MATLAB Simulink

Really??

SYMTA VISION
Formal Analysis of Timing Effects in CPS

Co-engineering Interaction Model

Plant, Control Problem, Functional requirements

- Analysis of plant dynamics (e.g. time constants)
- Specification of problem class
- Choice/derivation of control algorithm
- Discretization of control laws

Control Engineering (per control problem)

- Equations / Code
- Desired sampling rate (range)

Derive timing requirements

Timing structure of controller

Hardware Architecture, Tool Chain

- Integration of n control functions
- Mapping to cores
- Selection of scheduling strategy
- Assignment of scheduling parameters (offsets, priorities, ...)
- Assignment of execution orders and sequences

OK

NOK

Really!!

Real-time Engineering

MATLAB SIMULINK

SYMTA VISION

Arne Hamann | 9/22/2014 | © Robert Bosch GmbH 2014. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
Formal Analysis of Timing Effects in CPS

Electro Mechanic Braking System

Force

Position

$x_0$

$x$
Formal Analysis of Timing Effects in CPS

Electro Mechanic Braking System

1. Inactive
2. Positioning
3. Brake

Force

Position

$x_0$

$x$
Formal Analysis of Timing Effects in CPS

Simulink Plant Model

- Voltage
- DC Motor
- Rotating mass of rotor and spindle
- Gearing between rotational and translational mass
- Translational mass of the caliper including stiff spring for brake disk
- Caliper Position
- Braking Force
Formal Analysis of Timing Effects in CPS

Functional Requirements

- “Ready-to-brake” position $x_0 = 5$ mm
  - Preparation of braking system for applying brake force, no force closure

- Req. 1: Short response time
  - Reactiveness of the system
  - Caliper must be at $x_0$ after the braking request is issued within 20ms with a precision of 4%

- Req. 2: Small impulse before braking
  - Driver feels an abrupt deceleration
  - The caliper speed at contact must be below 2mm/s
  - Might be acceptable for braking, but not in other scenarios, e.g. disk wiping
Formal analysis using hybrid automatons and reachability analysis
Functional Verification with ZET* Assumption

Formal Analysis of Timing Effects in CPS

Closed-loop properties

Hybrid Automaton

Closed-loop properties

Plant

(discrete) Software

Simulation vs Reachability
- Simulation
  - approximative sample of single behavior
  - over finite time
- Reachability
  - over-approximative set-valued cover of all behaviors
  - over finite or infinite time

*ZET = Zero Execution Time

Trajectory planning $x_{des}$

Open-loop voltage control

Position deviation $\Delta x$

Position PI control

Caliper position $x$
Formal Analysis of Timing Effects in CPS

Functional Verification considering Timing

- Model Timing in Hybrid Automaton
  - When is data written / read
  - Non-deterministic model

- Possible models
  - Logical Execution Times
  - Arrival Curves
  - Typical Worst-Case Models
  - ...

- Drivers for choosing a model
  - Generality / analysis trade-off
  - Decision to simplify design for verifiability
  - Functional requirements
Formal Analysis of Timing Effects in CPS

Timing Structure – OSEK Systems

- Description of points in time where the plant is sampled, and where the actuation takes place
- Assumption: functionality implemented by a single process
- Example: Bosch Engine Management
  - Copy-in of required data at task release
  - Copy-out of produced data at process completion

Tasks are container for processes that contain the functional code

- Sampling Jitter
- Response Time Jitter

Patterns of control
- OK
- NOK
- Timing profile of controller
- Curve-based profile

Tasks are container for processes that contain the functional code

- Sample
- Actuate

Analysis of plant dynamics (e.g., time constants)
- Specification of performance requirements
- Design of control algorithms
- Design of control laws
- Timing requirements (i.e., latency)
- Integration of OSEK
- Real-time engineering
Formal Analysis of Timing Effects in CPS

Which Timing Model to choose?

⇒ LET?
- Trade Jitter against Latency → Determinism
- Great simplification of verification task
- Ok for “robust” control tasks based on exact models and little external disturbances

⇒ Arrival Curves?
- Precise model of possible system timing behavior
- Large space of possible timings
- Closed-loop verification very difficult

⇒ Typical Worst-Case Model!
- Allows for trade-off between both models
Typical Worst-Case Analysis

➤ Principle
- Identify typical bounds for the behavior of a system and how often the system may leave these bounds

➤ Output for each task
- a “safe” bound on its response times: SWCRT
- a typical bound: TWCRT
- a function \(err\) such that out of every \(k\) consecutive executions, at most \(err(k)\) response times may be larger than TWCRT

➤ Advantages
- Approach is computationally very efficient
- \textbf{m-out-of-k} constraints are easy to understand
- No assumptions w.r.t. dependencies
Formal Analysis of Timing Effects in CPS

Formal Analysis of Sporadic Overload

Scheduling policy: SPP (Static Priority Preemptive)

\[ T_1 > T_2 \]
Formal Analysis of Timing Effects in CPS

Modeling Sporadic Overload

\[ \delta_{over}^{(3)} - \delta_{over}^{(2)} \]

Worst case

Typical case

Overload

\[ \delta_{over}^{(3)} - \delta_{over}^{(2)} \]
Formal Analysis of Timing Effects in CPS

Formal Analysis of Sporadic Overload

Input:
1. a worst-case model of the system
2. a typical model ignoring the overload
3. a model of the overload

Analysis (for each task):
1. a busy window analysis of the worst-case model
   → Safe Worst-Case Response Time (SWCRT)
2. a busy window analysis of the typical-case model
   → Typical-Case Response Time (TWCRT)
3. a computation of the error model based on the result of 1. and the overload model
   → function err such that out of every k consecutive executions, at most err(k) response times may be larger than TWCRT
Formal Analysis of Timing Effects in CPS

Using TWCRT Model for Closed-loop Functional Verification

- Idea: Data is written to plant deterministically at TWCRT << WCRT (using LET)
  - Trade-off between determinism & functional requirements
- TWCRT misses are bounded by error function
- Scalable “discrete” timing model

<table>
<thead>
<tr>
<th># deadline misses</th>
<th>consecutive executions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
</tr>
<tr>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>56</td>
</tr>
</tbody>
</table>

(to be published RTSS 2014)
Formal Analysis of Timing Effects in CPS

Requirement 1: Response time

\[ x \text{ [dm]} \]

\[ t \text{ [ms]} \]

\(< 20 \text{ ms}\)
Requirement 2: Small impulse

- Current $I$ proportional to the caliper velocity
- Intersection reachable states with the plane of contact
- Bounds $[0.38, 0.99]$ satisfies the requirement 2.
Formal Analysis of Timing Effects in CPS

Conclusion

- Both control and real-time engineers have idealized system models for physical systems

- Functional integration effects are not considered by both disciplines
  - Integration effects are anticipated with overdesign
  - ...but even then, functional correctness cannot be guaranteed

- Reachability analysis for hybrid automatons is an adequate tool to verify closed loop properties under timing influences
  - Recent advances allow analysis of industrial strength applications

- One promising approach to close the gap between control and real-time system engineering
  - Verify correctness and performance of control software
  - Derive timing requirements for system synthesis
Formal Analysis of Timing Effects in CPS

Questions ???

Formal Analysis of Timing Effects on Closed-loop Properties of Cyber Physical Systems

Arne Hamann, Corporate Research, Robert Bosch GmbH

Joint work with: Matthias Wöhrle (Bosch), Goran Frehse (Université Joseph Fourier Grenoble), Sophie Quinton (INRIA Grenoble)