Hard real-time guarantees in cyber-physical systems

Author(s):
Kumar, Pratyush

Publication Date:
2014

Permanent Link:

https://doi.org/10.3929/ethz-a-010068802 →

Diss. ETH No. 21755

Hard Real-Time Guarantees in Cyber-Physical Systems

A thesis submitted to attain the degree of

Doctor of Sciences of ETH Zurich

(Dr. sc. ETH Zurich)

presented by

PRATYUSH KUMAR

Master of Technology,
Indian Institute of Technology Bombay

born May 4, 1987

citizen of India

accepted on the recommendation of

Prof. Dr. Lothar Thiele, examiner
Prof. Dr. Sanjoy Baruah, co-examiner

2014

Abstract

By integrating components for sensing, communicating, computing and actuating, Cyber-Physical Systems (CPSs) enable software applications to monitor and control events in the physical world. It is widely anticipated that CPSs will become pervasive in personal and industrial applications.

As deployed CPSs will impact safety of humans and infrastructure, certifying their correctness is imperative. For an important class of systems, correctness requires guaranteed timing properties. For instance, in an automatic stability program of an automobile, the worst-case end-to-end delay between sensing and actuating could be upper-bounded.

Analysis of such hard real-time guarantees in CPSs is inherently challenging, because the timing models exhibit variability due to multiple reasons. Firstly, as CPSs are distributed and heterogeneous, events do not arrive periodically. Secondly, on modern processors, resource availability can be non-uniform due to physical effects such as overheating or low energy supply. Thirdly, timing models can be uncertain either due to incorrect calibration or simultaneous analysis of multiple designs. Finally, due to complex components in such CPSs, such as caches, rare and transient phenomena can result in deviation from nominal timing models.

In three parts of the thesis, we present three templates of solutions to compute hard real-time guarantees in the presence of the said variability.

- Variability in arrival patterns of events can be absorbed by a run-time manager which monitors and adapts to incoming events. We illustrate this by compositionally building demand bound servers and cool-shapers from efficient constituent units.
- Variability in timing models can be bounded with analysis of sound abstractions which compactly represent the timing-critical traces of the system. We illustrate this with the analysis of temperature-controlled speed-scaling and the analysis of multiple designs within an Satisfiability Modulo Theory (SMT) solver.
- Variability due to rare and transient phenomena can be exported through richer guarantees to verify cross-layer objectives such as stability of a plant in a networked control system. We illustrate this by proposing and computing settling-time and overshoot metrics.

Zusammenfassung

Durch die Integration von Sensoren, Aktoren, Kommunikationsmodulen und Berechnungseneinheiten, ermöglichen Cyber-physische Systeme Softwareanwendungen für die Überwachung und Steuerung von Ereignissen der physischen Welt. Es wird allgemein erwartet, dass in Zukunft Cyber-physische Systeme in personenbezogenen und industriellen Anwendungen allgegenwärtig sein werden.

Da Cyber-physische Systeme die Sicherheit von Mensch und Infrastruktur beeinflussen werden, ist die Bescheinigung ihrer Korrektheit zwingend notwendig. Für eine wichtige Klasse von Systemen erfordert Korrektheit garantierte Zeiteigenschaften. Beispielsweise könnte man so für das automatisierte Stabilitätsprogramm eines Autos, eine obere Grenze für die Worstcase Verzögerung zwischen Sensor und Aktor angeben.

Die Analyse solcher harten Echtzeitgarantien in Cyber-physischen Systemen ist von Natur aus eine Herausforderung, da Timing-Modelle wegen unterschiedlichen Gründen Variabilität aufweisen.

Erstens, da Cyber-physische Systeme verteilt und heterogen sind, treten Ereignisse unregelmässig auf. Zweitens, auf modernen Prozessoren kann die Verfügbarkeit von Ressourcen, aufgrund von physikalischen Effekten wie Überhitzung oder niedrige Energieversorgung, ungleichförmig sein. Drittens, Timing-Modelle können Unsicherheiten aufweisen, welche entweder durch eine falsche Kalibrierung oder die gleichzeitige Analyse von mehreren Entwürfen entstehen. Schliesslich können seltene und vorübergehende Phänomene, wegen den komplexen Bauteilen in Cyber-physischen Systemen, wie zum Beispiel Zwischenspeichern, zu Abweichungen der Timing-Modelle führen.

In den drei Teilen dieser Arbeit präsentieren wir drei Lösungsvorlagen für die Berechnung harter Echtzeitgarantien im Beisein der oben genannten Variabilität.

- Die Variabilität der Ankunftszeiten von Ereignissen kann von einem Laufzeit-Manager absorbiert werden, der eingehende Ereignisse überwacht und sich entsprechend anpasst. Wir veranschaulichen dies durch den Aufbau eines Demand-Bound-Servers und Cool-

Shapers, welche aus einzelnen effizienten Bauteilen zusammengesetzt sind.

- Die Variabilität der Timing-Modelle kann durch die Analyse von Abstraktionen eingegrenzt werden, welche kompakt die zeitkritischen Abläufe des Systems darstellen. Wir veranschaulichen dies mit der Analyse von einer temperaturgesteuerten Geschwindigkeitsskalierung und der Analyse von mehreren Entwürfen mit einem Satisfiability Modulo Theory (SMT) Löser.
- Variabilität, die durch seltene und vorübergehende Phänomene entsteht, kann durch zusätzliche Garantien ausgelagert werden um so Cross-Layer-Ziele zu verifizieren, wie zum Beispiel die Stabilität einer Anlage in einem vernetzten Kontrollsystem. Wir veranschaulichen dies durch die Empfehlung und Berechnung von Einschwingzeiten und Übersteuerungsmetriken.