DISS. ETH NO. 24023

Design and Optimization of Mixed-Criticality Systems

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH
(Dr. sc. ETH Zurich)

presented by
PENGCHENG HUANG
Master of Science,
Delft University of Technology

born on May 26, 1987
citizen of China

accepted on the recommendation of
Prof. Dr. Lothar Thiele, examiner
Prof. Dr. Alan Burns, co-examiner

2016

Abstract

Mixed-Criticality is emerging as a significant trend for safety-critical systems, especially in automotive and avionics industries. Conventionally, those systems are designed as multiple sub-systems of *distinct* criticality or importance levels. With the ever-increasing demand of system functionalities and the shift of the semiconductor industry to more powerful (multi-core) platforms, consolidating/mixing functionalities of different criticality levels in a common hosting platform is appealing – system costs induced by size, weight and power consumptions could be potentially greatly reduced in the mixed-criticality setting.

The benefits brought by mixed-criticality systems are, however, accompanied by a multitude of new challenges. Most noticeably, due to resource sharing, functionalities of different criticality levels can interfere with each other, jeopardizing their guarantees made in isolation. To address this, new mixed-criticality models/protocols and corresponding scheduling techniques need to be developed to provide adequate isolation among criticality levels, and their limits (as well as potential extensions) need to be understood. Many traditional design issues for conventional embedded and/or safety-critical systems need to be rethought in the mixed-criticality era. For example, in addition to common timing threats considered for time-critical systems, hardware/software faults also need to be considered in the design of real-time mixed-safety-critical systems. In order to increase the system power efficiency, it is necessary to extend conventional energy minimization techniques to emerging mixed-criticality applications while considering the peculiarities of such systems.

As a step towards solving the above challenges, this thesis presents a whole stack of solutions to model, design and optimize mixed-criticality systems, in areas regarding real-time, fault-tolerance and energy-efficiency. Specifically, we make three main contributions:

1 We design the first mixed-criticality models to improve the service guarantee for less critical tasks in urgent scenarios – existing solutions commonly assume to drop all those tasks when any critical task overruns, which could be hardly acceptable in practice. In particular, we propose service adaptation, detailed modeling through interference constraint graphs, and processor over-clocking to adaptively degrade the system service in urgent scenarios. We show how common scheduling techniques like fixed-priority (FP)

and earliest deadline first (EDF) can be extended under those models and demonstrate considerable performance improvements compared to existing solutions. To further understand the limit of existing mixed-criticality models in line with industrial practices (i.e., with static temporal isolation among criticality levels), we present optimal scheduling techniques and we theoretically quantify the schedulability loss of those models.

2 We present the first mixed-criticality framework, where fault-tolerance, real-time requirements and runtime adaptation are jointly considered to achieve a safe system design. Assuming hardware/software faults, we adopt task re-execution (single-core) and replication (multi-core) as our fault-tolerance techniques and explicitly follow safety standards to model system safety requirements on different criticality levels. To further deal with urgent scenarios where critical tasks do not succeed after a certain number of trials, we propose runtime adaptations to reallocate system resources to critical tasks in such scenarios. Based on this, we present fault-tolerant mixed-criticality scheduling techniques and corresponding analysis techniques to meet both, safety and real-time requirements. Our solutions work on single-core and multi-core platforms, demonstrating the advantages of runtime adaptations and revealing important findings on the impact of commonly assumed mixed-criticality reconfigurations on the system feasibility.

3 We develop the first dynamic voltage and frequency scaling (DVFS) techniques to improve energy efficiency for mixed-criticality systems. We show that fundamental trade-offs exist for this problem: DVFS can help the system to speedup in order to overcome the urgent scenarios where critical tasks overrun, which further allows the system to relax (slow down) and save dynamic energy in nominal scenarios where tasks do not overrun. Assuming EDF based scheduling, we present optimal and heuristic solutions in a general setting firstly on a single-core, considering both leakage and dynamic energy consumptions and all different system operation scenarios. We then develop energy-aware mixed-criticality task mapping techniques to extend our single-core solutions to multi-core platforms. Our solutions demonstrate considerable energy savings for both synthetic task sets and a realistic industrial use-case, while revealing a rather surprising finding – the industrial best practice of spatially isolating different criticality levels almost has comparable energy savings to mixing them on each core.

Zusammenfassung

Mixed-Criticality ist ein bedeutender Trend im Bereich sicherheitskritischer Systeme, allem voran in der Automobil- und Avionikindustrie. Konventionelle Systeme bestehen aus mehreren Teilsystemen, welche *unterschiedliche* Kritikalitäts-/Wichtigkeitsniveaus abdecken. Mit steigender Nachfrage nach erweiterter Systemfunktionalität und der Verlagerung der Prozessorindustrie auf leistungsfähigere (Multi-Core) Plattformen ist es vielversprechend die Funktionalitäten unterschiedlicher Kritikalitätsniveaus auf einer gemeinsamen Plattform zu konsolidieren. Durch Grösse, Gewicht und Energieverbrauch bedingte Systemkosten lassen sich in einem Mixed-Criticality Setting möglicherweise stark reduzieren.

Die Vorteile, welche Mixed-Criticality Systeme bieten, werden jedoch von einer Vielzahl neuer Herausforderungen begleitet. Besonders durch Ressourcen-Sharing können sich verschiedene Kritikalitätsniveaus gegenseitig stören, obwohl durch Isolation diese gegenseitige Beeinflussung ausgeschlossen werden soll. Um diese Probleme zu adressieren, müssen neue Mixed-Criticality Modelle und Protokolle, sowie entsprechende Scheduling-Techniken entwickelt und deren Grenzen (und mögliche Erweiterungen) verstanden werden um genügende Isolation zwischen den unterschiedlichen Kritikalitätsniveaus zu garantieren. Viele typischen Designfragen konventioneller eingebetteter und/oder sicherheitskritischer Systeme müssen in der Mixed-Criticality Ära überdacht werden. So müssen zum Beispiel zusätzlich zu den üblichen Tasküberlauf in zeitkritischen Systemen auch Hardware- und Software-Fehler in der Designphase von Echtzeit Mixed-Criticality Systemen bedacht werden. Um ebenfalls die Energieeffizienz solcher Systeme zu verbessern, ist es ebenso notwendig konventionelle Energiesparmechanismen für zukünftige Mixed-Criticality Systeme zu erweitern.

Diese Disseration stellt einen ersten Schritt zur Lösung dieser Probleme dar. Dabei werden eine Reihe von Lösungen zur Modellierung, dem Design und der Optimierung von Mixed-Criticality Systemen in den Bereichen Echtzeitverarbeitung, Fehlertoleranz und Energieeffizienz präsentiert. Im Einzelnen werden folgende Beiträge gemacht:

1 Wir entwerfen die ersten Mixed-Criticality Modelle welche die Servicegarantie weniger kritischer Tasks in dringenden Situationen verbessern. Im Gegensatz dazu gehen bestehende Lösungen davon aus, dass weniger kritische Tasks automatisch abgebrochen werden sobald

ein kritischer Task überläuft, was in der Praxis kaum umsetzbar ist. Insbesondere schlagen wir dynamische Serviceadaptierung, detaillierterer Modellierung mittels Interferenz Bedingungsgraphen und Prozessorübertaktung vor, um den Systemservice in dringenden Situationen zu adaptieren. Wir zeigen auf wie bekannte Schedulingalgorithmen wie Fixed-Priority (FP) und Earliest-Deadline-First (EDF) mithilfe dieser Modelle erweitert werden können und demonstrieren dass diese die Performance gegenüber bestehenden Lösungen erheblich verbessern. Ebenso präsentieren wir optimale Schedulingtechniken und quantifizieren die Einbussen auf die Schedulability um die Einschränkungen bestehender Mixed-Criticality Modellen im Zusammenhang mit der Industriepraxis, wie zum Beispiel zeitliche Isolation der Kritikaliätsniveaus, zu verstehen.

2 Wir präsentieren das erste Mixed-Criticality Framework welches Echtzeit-Anforderungen und Serviceanpassung zur Laufzeit gemeinsam betrachtet um ein sicheres Systemdesign zu erzielen. Unter der Annahme von Hardware- und Softwarefehlern Übernehmen wir die Techniken Task-Wiederausführung (Single-Core) und Replikation (Multi-Core) um Fehlertoleranz zu garantieren und folgen den strikten Sicherheitsstandards um die Sicherheitsanforderungen der verschiedenen Kritikalitätsniveaus zu modellieren. Weiter behandeln wir dringende Situationen in welchen kritische Tasks auch nach einigen Wiederausführungen nicht erfolgreich abgearbeitet wurden. In diesen Fällen schlagen wir vor dynamisch weitere System-Ressourcen für diese kritischen Tasks zu allozieren. Darauf aufbauend präsentieren wir fehlertolerante Mixed-Cricicality Schedulingalgorithmen and entsprechende Analysetechniken um Sicherheits- und Echtzeitanforderungen zu erfüllen. Die gezeigte Lösung arbeitet sowohl auf Single-Core als auch Multi-Core Systemen und liefert wichtige Erkenntnisse über den Einfluss typischer Rekonfigurationsmassnahmen auf die Umsetzbarkeit von Mixed-Criticality Systemen.

3 Wir entwickeln die erste dynamische Spannungs- und Frequenzskalierung (Dynamic Voltage and Frequency Scaling, DVFS) Technik für Mixed-Criticality Systeme und zeigen auf, welche grundlegenden Kompromisse für dieses Problem getroffen werden müssen: DVFS kann helfen die Ausführung zu beschleunigen um dringende Situationen zu überwinden und hilft zudem das System zu verlangsamen um Energie einzusparen wenn kritische Tasks keine erhöhten Ausführungszeiten haben. Wir präsentieren eine optimale und heuristische Lösung für EDF basiertes Scheduling für Single-Core Architekturen unter Einbeziehung von Leakage und dynamischem Energieverbrauch und

allen möglichen Systemzuständen. Wir entwicklen energiebewusste Mixed-Criticality Task-Mapping Algorithmen zur Erweiterung der Single-Core Lösung auf Multi-Core Plattformen. Die Evaluation unserer Lösung zeigt signifikante Energieeinsparungen sowohl für synthetische Task-Sets, als auch realistische industrielle Anwendungen. Interessanterweise zeigt die Anwendung der gleichen Massnahmen auf die industrielle Best Practice räumlicher Isolation annähernd die gleichen Energieeinsparungen.