Design of Mixed-Criticality Applications on Distributed Real-Time Systems

A mixed-criticality system implements applications of different safety-criticality levels onto the same platform. In such cases, the certification standards require that applications of different criticality levels are protected so they cannot influence each other. Otherwise, all tasks have to be developed and certified according to the highest criticality level, dramatically increasing the development costs. In this thesis we consider mixed-criticality real-time applications implemented on distributed partitioned architectures.

Partitioned architectures use temporal and spatial separation mechanisms to ensure that applications of different criticality levels do not interfere with each other. With temporal partitioning, each application is allowed to run only within predefined time slots, allocated on each processor. The sequence of time slots for all the applications on a processor are grouped within a Major Frame, which is repeated periodically. Each partition can have its own scheduling policy; we have considered non-preemptive static cyclic scheduling and fixed-priority preemptive scheduling policies. We assume that the communication network implements the TTEthernet protocol, which supports Time-Triggered (TT) messages transmitted based on static schedule tables, Rate Constrained (RC) messages with bounded end-to-end delay, and Best-Effort (BE) messages, for which no timing guarantees are provided. TTEthernet offers spatial separation for mixed-criticality messages through the concept of virtual links, and temporal separation, enforced through schedule tables for TT messages and bandwidth allocation for RC messages.

The objective of this thesis is to develop methods and tools for distributed mixed-criticality real-time systems. At the processor level, we are interested to determine (i) the mapping of tasks to processors, (ii) the assignment of tasks to partitions, (iii) the decomposition of tasks into redundant lower criticality tasks, (iv) the sequence and size of the partition time slots on each processor and (v) the schedule tables, such that all the applications are schedulable and the development and certification costs are minimized. We have proposed Simulated Annealing and Tabu Search metaheuristics to solve these optimization problems. The proposed algorithms have been evaluated using several benchmarks.

At the communication network level, we are interested in the design optimization of TTEthernet networks used to transmit mixed-criticality messages. Given the set of TT and RC messages, and the topology of the network, we are interested to optimize (i) the packing of messages in frames, (ii) the assignment of frames to virtual links, (iii) the routing of virtual links and (iv) the TT static schedules, such that all frames are schedulable and the worst-case end-to-end delay of the RC messages is minimized. We have proposed a Tabu Search-based metaheuristic for this optimization problem.

The proposed algorithm has been evaluated using several benchmarks. The optimization approaches have also been evaluated using realistic aerospace case studies. In this context, we have shown how to extend the proposed optimization frameworks to also take into account quality of service constraints. For TTEthernet networks, we have also proposed a topology selection method to reduce the cost of the architecture.
Design Optimization of Mixed-Criticality Real-Time Embedded Systems

In this article, we are interested in implementing mixed-criticality real-time embedded applications on a given heterogeneous distributed architecture. Applications have different criticality levels, captured by their Safety-Integrity Level (SIL), and are scheduled using static-cyclic scheduling. According to certification standards, mixed-criticality tasks can be integrated onto the same architecture only if there is enough spatial and temporal separation among them. We consider that the separation is provided by partitioning, such that applications run in separate partitions, and each partition is allocated several time slots on a processor. Tasks of different SILs can share a partition only if they are all elevated to the highest SIL among them. Such elevation leads to increased development costs, which increase dramatically with each SIL. Tasks of higher SILs can be decomposed into redundant structures of lower SIL tasks. We are interested to determine (i) the mapping of tasks to processors, (ii) the assignment of tasks to partitions, (iii) the decomposition of tasks into redundant lower SIL tasks, (iv) the sequence and size of the partition time slots on each processor, and (v) the schedule tables, such that all the applications are schedulable and the development costs are minimized. We have proposed a Tabu Search-based approach to solve this optimization problem. The proposed algorithm has been evaluated using several synthetic and real-life benchmarks.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Tamas-Selicean, D. (Intern), Pop, P. (Intern)
Number of pages: 29
Publication date: 2015
Main Research Area: Technical/natural sciences

Publications information
Journal: ACM Transactions on Embedded Computing Systems
Volume: 14
Issue number: 3
Article number: 50
ISSN (Print): 1539-9087
Ratings:
BFI (2018): BFI-level 1
BFI (2017): BFI-level 1
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.377 SNIP 1.145 CiteScore 1.69
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.322 SNIP 0.895 CiteScore 1.28
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.233 SNIP 0.708 CiteScore 0.8
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.31 SNIP 1.095 CiteScore 1.05
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.329 SNIP 1.257 CiteScore 1.48
Design optimization of TTEthernet-based distributed real-time systems

Many safety-critical real-time applications are implemented using distributed architectures, composed of heterogeneous processing elements interconnected in a network. Our focus in this paper is on the TTEthernet protocol, a deterministic, synchronized and congestion-free network protocol based on the Ethernet standard and compliant with the ARINC 664 Specification Part 7. TTEthernet is highly suitable for safety-critical real-time applications since it offers separation for messages using the concept of virtual links and supports three time-criticality classes: Time-Triggered (TT), Rate-Constrained (RC) and Best-Effort. In this paper we are interested in the design optimization of TTEthernet networks used to transmit real-time application messages. Given the set of TT and RC messages, and the topology of the network, our approach optimizes the packing of messages in frames, the assignment of frames to virtual links, the routing of virtual links and the TT static schedules, such that all frames are schedulable and the worst-case end-to-end delay of the RC messages is minimized. We propose a Tabu Search-based metaheuristic for this optimization problem. The proposed algorithm has been evaluated using several benchmarks.
Fault-Tolerant Topology Selection for TT-Ethernet Networks

Many safety-critical real-time applications are implemented using distributed architectures, composed of heterogeneous processing elements (PEs) interconnected in a network. In this paper, we are interested in the TT-Ethernet protocol, which is a deterministic, synchronized and congestion-free network protocol based on the IEEE 802.3 Ethernet standard and compliant with ARINC 664p7. TT-Ethernet supports three types of traffic: static time-triggered (TT) traffic and dynamic traffic, which is further subdivided into Rate Constrained (RC) traffic that has bounded end-to-end latencies, and Best-Effort (BE) traffic, for which no timing guarantees are provided. TT-Ethernet offers spatial separation through the concept of virtual links (VLs), and temporal separation, through schedule tables for TT messages and bandwidth allocation for RC messages. Given a set of PEs, we are interested to determine a fault-tolerant network topology, consisting of redundant physical links and network switches, such that the architecture cost is minimized, the applications are fault-tolerant to a given number of permanent faults occurring in the communication network, and the timing constraints of the TT and RC messages are satisfied. Deciding on a fault-tolerant topology means (i) deciding on the number of network switches, (ii) the physical links and the network topology, (iii) the routing of VLs on top of the physical network, (iv) the assignment of frames to VLs and (v) the schedule tables for the TT frames. We propose a Simulated Annealing meta-heuristic to solve this optimization problem. The proposed approach has been evaluated using a synthetic benchmark and a space case study, based on the Orion Crew Exploration Vehicle.
Timing Analysis of Rate Constrained Traffic for the TTEthernet Communication Protocol

Ethernet is a low-cost communication solution offering high transmission speeds. Although its applications extend beyond computer networking, Ethernet is not suitable for real-time and safety-critical systems. To alleviate this, several real-time Ethernet-based communication protocols have been proposed, such as TTEthernet, which is the focus of this paper. TTEthernet is suitable for mixed-criticality systems both in the safety and temporal domain. TTEthernet offers three traffic classes: static time-triggered (TT) traffic, dynamic traffic with bounded transmission rate (called "Rate Constrained", RC), and unbounded dynamic traffic ("Best-Effort", BE). In this paper we propose a novel worst-case end-to-end delay analysis of the RC traffic for TTEthernet systems. The proposed technique considerably reduces the pessimism of the analysis, compared to existing approaches. We have evaluated the new analysis using several test cases.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, TTTech Computertechnik AG
Authors: Tamas-Selicean, D. (Intern), Pop, P. (Intern), Steiner, W. (Ekstern)
Number of pages: 2
Pages: 223 - 224
Publication date: 2014

Host publication information

Title of host publication: Proceedings of the 18th International Symposium on Real-Time Distributed Computing (ISORC 2015)
Publisher: IEEE
ISBN (Print): 978-1-4799-8781-8
BFI conference series: Object-Oriented Real-Time Distributed Computing (5000415)
Main Research Area: Technical/natural sciences
DOIs: 10.1109/ISORC.2015.32
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015
Optimization of TTEthernet Networks to Support Best-Effort Traffic

This paper focuses on the optimization of the TTEthernet communication protocol, which offers three traffic classes: time-triggered (TT), sent according to static schedules, rate-constrained (RC) that has bounded end-to-end latency, and best-effort (BE), the classic Ethernet traffic, with no timing guarantees. In our earlier work we have proposed an optimization approach named DOTTS that performs the routing, scheduling and packing/fragmenting of TT and RC messages, such that the TT and RC traffic is schedulable. Although backwards compatibility with classic Ethernet networks is one of TTEthernet’s strong points, there is little research on this topic. However, in this paper, we extend our DOTTS optimization approach to optimize TTEthernet networks, such that not only the TT and RC messages are schedulable, but we also maximize the available bandwidth for BE messages. The proposed optimization has been evaluated on a space application case study.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Tamas-Selicean, D. (Intern), Pop, P. (Intern)
Pages: 1-4
Publication date: 2014

Fourier Transform Spectrometer Controller for Partitioned Architectures

The current trend in spacecraft computing is to integrate applications of different criticality levels on the same platform using no separation. This approach increases the complexity of the development, verification and integration processes, with an impact on the whole system life cycle. Researchers at ESA and NASA advocated for the use of partitioned architecture to reduce this complexity. Partitioned architectures rely on platform mechanisms to provide robust temporal and spatial separation between applications. Such architectures have been successfully implemented in several industries, such as avionics and automotive. In this paper we investigate the challenges of developing and the benefits of integrating a scientific instrument, namely a Fourier Transform Spectrometer, in such a partitioned architecture.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, NASA Jet Propulsion Laboratory, Designs & Prototypes Ltd., Quant Engineering LLC
Analysis and Optimization of Mixed-Criticality Applications on Partitioned Distributed Architectures

In this paper we are interested in mixed-criticality applications implemented using distributed heterogenous architectures, composed of processing elements (PEs) interconnected using the TTEthernet protocol. At the PE-level, we use partitioning, such that each application is allowed to run only within predefined time slots, allocated on each processor. At the communication-level, TTEthernet uses the concepts of virtual links for the separation of mixed-criticality messages. TTEthernet integrates three types of traffic: Time-Triggered (TT) messages, transmitted based on schedule tables, Rate Constrained (RC) messages, transmitted if there are no TT messages, and Best Effort (BE) messages. We assume that applications are scheduled using Static Cyclic Scheduling (SCS) or Fixed-Priority Preemptive Scheduling (FPS). We are interested in analysis and optimization methods and tools, which decide the mapping of tasks to PEs, the sequence and length of the time partitions on each PE and the schedule tables of the SCS tasks and TT messages, such that the applications are schedulable and the response times of FPS tasks and RC messages is minimized. We have proposed a Tabu Search-based meta-heuristic to solve this optimization problem, which has been evaluated using several benchmarks.

Synthesis of Communication Schedules for TTEthernet-Based Mixed-Criticality Systems

In this paper we are interested in safety-critical distributed systems, composed of heterogeneous processing elements interconnected using the TTEthernet protocol. We address hard real-time mixed-criticality applications, which may have different criticality levels, and we focus on the optimization of the communication configuration. TTEthernet integrates three types of traffic: Time-Triggered (TT) messages, Event-Triggered (ET) messages with bounded end-to-end delay, also called Rate Constrained (RC) messages, and Best-Effort (BE) messages, for which no timing guarantees are provided. TT messages are transmitted based on static schedule tables, and have the highest priority. RC messages are transmitted if there are no TT messages, and BE traffic has the lowest priority. TT and RC traffic can carry safety-critical messages, while BE messages are non-critical. Mixed-criticality tasks and messages can be integrated onto the same architecture only if there is enough spatial and temporal separation among them. TTEthernet offers spatial separation for mixed-criticality messages through the concept of virtual links, and temporal separation, enforced through schedule tables for TT messages and bandwidth allocation for RC messages. Given the set of mixed-criticality messages in the system
and the topology of the virtual links on which the messages are transmitted, we are interested to synthesize offline the static schedules for the TT messages, such that the deadlines for the TT and RC messages are satisfied, and the end-to-end delay of the RC traffic is minimized. We have proposed a Tabu Search-based approach to solve this optimization problem. The proposed algorithm has been evaluated using several benchmarks.

**General information**

State: Published  
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, Computer Science and Engineering, TTTech Computertechnik AG  
Authors: Tamas-Selicean, D. (Intern), Pop, P. (Intern), Steiner, W. (Ekstern)  
Pages: 473-482  
Publication date: 2012

**Host publication information**

Title of host publication: CODES+ISSS '12 : Proceedings of the eighth IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis  
Publisher: Association for Computing Machinery  
ISBN (Print): 978-1-4503-1426-8  
BFI conference series: International Conference on Hardware Software Codesign (5000325)  
Main Research Area: Technical/natural sciences  
Conference: 8th IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis (CODES+ISSS '12), Tampere, Finland, 07/10/2012 - 07/10/2012  
DOIs:  
10.1145/2380445.2380518  
Source: dtu  
Source-ID: u::5858  
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

**Task Mapping and Partition Allocation for Mixed-Criticality Real-Time Systems**

In this paper we address the mapping of mixed-criticality hard real-time applications on distributed embedded architectures. We assume that the architecture provides both spatial and temporal partitioning, thus enforcing enough separation between applications. With temporal partitioning, each application runs in a separate partition, and each partition is allocated several time slots on the processors where the application is mapped. The sequence of time slots for all the applications on a processor are grouped within a Major Frame, which is repeated periodically. We assume that the applications are scheduled using static-cyclic scheduling. We are interested to determine the task mapping to processors, and the sequence and size of the time slots within the Major Frame on each processor, such that the applications are schedulable. We have proposed a Tabu Search-based approach to solve this optimization problem. The proposed algorithm has been evaluated using several synthetic and real-life benchmarks.

**General information**

State: Published  
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling  
Authors: Tamas-Selicean, D. (Intern), Pop, P. (Intern)  
Publication date: 2012

**Host publication information**

Title of host publication: 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC)  
Publisher: IEEE  
Main Research Area: Technical/natural sciences  
Electronic versions:  
main.pdf  
DOIs:  
10.1109/PRDC.2011.42  
Links:  
http://prdc.dependability.org/2011/  
Source: orbit  
Source-ID: 312711  
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012
Timing Analysis of Mixed-Criticality Hard Real-Time Applications Implemented on Distributed Partitioned Architectures
In this paper we are interested in the timing analysis of mixed-criticality embedded real-time applications mapped on distributed heterogeneous architectures. Mixed-criticality tasks can be integrated onto the same architecture only if there is enough spatial and temporal separation among them. We consider that the separation is provided by partitioning, such that applications run in separate partitions, and each partition is allocated several time slots on a processor. Each partition can have its own scheduling policy. We are interested to determine the worst-case response times of tasks scheduled in partitions using fixed-priority preemptive scheduling. We have extended the state-of-the-art algorithms for schedulability analysis to take into account the partitions. The proposed algorithm has been evaluated using several synthetic and real-life benchmarks.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Software Engineering, Technical University of Denmark
Authors: Marinescu, S. O. (Ekstern), Tamas-Selicean, D. (Intern), Acretoaie, V. (Intern), Pop, P. (Intern)
Number of pages: 4
Publication date: 2012
Main Research Area: Technical/natural sciences
Electronic versions:
etfa2012.pdf
Source: dtu
Source-ID: u::6870
Publication: Research - peer-review › Paper – Annual report year: 2013

Design Optimization of Mixed-Criticality Real-Time Applications on Cost-Constrained Partitioned Architectures
In this paper we are interested to implement mixed-criticality hard real-time applications on a given heterogeneous distributed architecture. Applications have different criticality levels, captured by their Safety-Integrity Level (SIL), and are scheduled using static-cyclic scheduling. Mixed-criticality tasks can be integrated onto the same architecture only if there is enough spatial and temporal separation among them. We consider that the separation is provided by partitioning, such that applications run in separate partitions, and each partition is allocated several time slots on a processor. Tasks of different SILs can share a partition only if they are all elevated to the highest SIL among them. Such elevation leads to increased development costs. We are interested to determine (i) the mapping of tasks to processors, (ii) the assignment of tasks to partitions, (iii) the sequence and size of the time slots on each processor and (iv) the schedule tables, such that all the applications are schedulable and the development costs are minimized. We have proposed a Tabu Search-based approach to solve this optimization problem. The proposed algorithm has been evaluated using several synthetic and real-life benchmarks.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Tamas-Selicean, D. (Intern), Pop, P. (Intern)
Pages: 24-33
Publication date: 2011
Host publication information
Title of host publication: 2011 IEEE 32nd Real-Time Systems Symposium (RTSS)
Publisher: IEEE
ISBN (Print): 978-1-4577-2000-0
Main Research Area: Technical/natural sciences
Conference: IEEE Real-Time Systems Symposium, Vienna, Austria, 01/01/2011
Electronic versions:
dota_rtss11.pdf
DOIs: 10.1109/RTSS.2011.11
Links: http://www.rtss.org/
Source: orbit
Source-ID: 312709
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

Optimization of Time-Partitions for Mixed-Criticality Real-Time Distributed Embedded Systems
In this paper we are interested in mixed-criticality embedded real-time applications mapped on distributed heterogeneous architectures. The architecture provides both spatial and temporal partitioning, thus enforcing enough separation for the
critical applications. With temporal partitioning, each application is allowed to run only within predefined time slots, allocated on each processor. The sequence of time slots for all the applications on a processor are grouped within a Major Frame, which is repeated periodically. We assume that the safety-critical applications (on all criticality levels) are scheduled using static-cyclic scheduling and the noncritical applications are scheduled using fixed-priority preemptive scheduling. We consider that each application runs in a separate partition, and each partition is allocated several time slots on the processors where the application is mapped. We are interested to determine the sequence and size of the time slots within the Major Frame on each processor such that both the safety-critical and non-critical applications are schedulable. We have proposed a Simulated Annealing-based approach to solve this optimization problem. The proposed algorithm has been evaluated using several synthetic and real-life benchmarks.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Tamas-Selicean, D. (Intern), Pop, P. (Intern)
Publication date: 2011

Host publication information
Title of host publication: 2011 14th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW)
Publisher: IEEE
ISBN (Print): 978-1-4577-0303-4
Main Research Area: Technical/natural sciences
Conference: IEEE International Symposium on Object/Component/Service-oriented Real-time Distributed Computing, Newport Beach, California, USA, 01/01/2011
Real-time systems, Temporal partitioning, Mixed-criticality
DOIs: 10.1109/ISORCW.2011.11
Links: http://dream.eng.uci.edu/isorc2011/
Source: orbit
Source-ID: 278107
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

Projects:

Synthesis of Mixed-Criticality Applications on Multi-Core Systems to Reduce Certification Costs
Department of Applied Mathematics and Computer Science
Period: 01/09/2010 → 20/03/2014
Number of participants: 6
Phd Student: Tamas-Selicean, Domitian (Intern)
Supervisor: Madsen, Jan (Intern)
Main Supervisor: Pop, Paul (Intern)
Examiner: Schoeberl, Martin (Intern)
Ademaj, Astrit (Ekstern)
Chakraborty, Samarjit (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet
Project: PhD