

## **Emprego de Medição na Estimação do Tempo de Execução no Pior Caso para Sistemas de Tempo Real Crítico**

Projeto de Dissertação de Mestrado

Orientador: Rômulo Silva de Oliveira

Co-Orientador: Luís Fernando Arcaro (IFSC)

### **1. Introdução**

Sistemas computacionais de tempo real são identificados como aqueles sistemas computacionais submetidos a requisitos de natureza temporal. Nesses sistemas, os resultados devem estar corretos não somente do ponto de vista lógico, mas também devem ser gerados obedecendo aos prazos (*deadlines*) estabelecidos. As falhas de natureza temporal nesses sistemas são, em alguns casos, consideradas críticas no que diz respeito às suas consequências.

Na literatura, os sistemas de tempo real são classificados conforme a criticalidade dos seus requisitos temporais. Nos sistemas tempo real críticos (*hard real-time*) o não atendimento de um requisito temporal pode resultar em consequências catastróficas tanto no sentido econômico quanto em vidas humanas. Quando os requisitos temporais não são críticos (*soft real-time*) eles apenas descrevem o comportamento desejado. O não atendimento de tais requisitos reduz a utilidade da aplicação, mas não a elimina completamente nem resulta em consequências catastróficas.

Sistemas de tempo real são uma tecnologia fundamental para a instrumentação necessária no contexto da Indústria 4.0. O desenvolvimento de sistemas para condicionamento analógico de sinais visando a realização de medições, o desenvolvimento de sistemas embarcados integrando instrumentos e microcontroladores, e a integração desses com a Internet/nuvem, são atividades fundamentais. A evolução industrial pressupõe a disseminação de sistemas distribuídos que trocam informação entre si através de redes de comunicação digital de alto desempenho que são conhecidos na literatura como Sistemas de Controle em Rede (NCS – Networked Control Systems).

Para que seja possível garantir a escalonabilidade do sistema, ou seja, que todos seus prazos são atendidos, algumas premissas são necessárias. A carga computacional gerada pela aplicação deve ser limitada e conhecida em tempo de projeto, pois é impossível garantir uma aplicação cujas tarefas são desconhecidas. Essa premissa é conhecida como hipótese de carga (*load hypothesis*). Da mesma forma, é impossível dar qualquer garantia se puderem acontecer faltas indiscriminadas no sistema, incluindo uma pane no processador. Dessa forma, a garantia é dada a partir de uma hipótese de faltas (*fault hypothesis*), a qual delimita as faltas que poderão ocorrer sem perda da garantia. Ou seja, que faltas serão toleradas a partir de uma perspectiva temporal. Tipicamente, tolerância a faltas (*fault tolerance*) é obtida a partir de algum tipo de redundância.

Qualquer abordagem que pretenda fornecer garantia para os *deadlines* precisa conhecer o comportamento do sistema no pior caso, tanto do *software* quanto do *hardware*. Isso porque os *deadlines* deverão ser cumpridos mesmo nos cenários mais desfavoráveis para a aplicação. Isso significa supor o pior caso, incluindo: o pior fluxo de controle para cada tarefa, o pior cenário de sincronização entre tarefas (exclusão mútua, etc.), os piores dados de entrada, a pior combinação de eventos externos (interrupções, sensores, etc.), o pior comportamento das *caches* internas e externas do *hardware*, o pior comportamento do processador (*pipeline*, barramentos, etc.), ou seja, um cenário composto pela pior combinação possível de eventos. No cenário de pior caso, teremos o tempo de execução no pior caso (*WCET – Worst-Case Execution Time*) para cada tarefa

individualmente, assim como o tempo de resposta no pior caso (*WCRT – Worst-Case Response Time*), esse último combinando a execução das várias tarefas.

A introdução de elementos cada vez mais complexos e cujo comportamento temporal não é determinístico nas arquiteturas computacionais modernas, como memórias *cache*, *pipelines* superescalares e mecanismos de predição de fluxo (*branch prediction*), acaba por dificultar ou até mesmo impossibilitar a determinação do tempo máximo de execução de uma tarefa. Nesse contexto, a determinação do tempo de execução no pior caso (*WCET*) é um elemento essencial para a análise de escalonabilidade, especialmente em sistemas de tempo real críticos.

O método de medições de tempo de execução consiste em executar uma tarefa de *software*, ou partes dela, para um conjunto de entradas, em um *hardware* específico ou em um simulador. Assim, múltiplos tempos de operação dos diferentes componentes e procedimentos definidos em cada tarefa são avaliados. O tempo de execução mínimo e máximo, a distribuição desses tempos, ou também uma combinação entre os tempos de operação de diferentes segmentos de código são calculados.

Utilizando medição é difícil determinar se os valores obtidos são seguros, ou seja, é difícil garantir que o maior tempo de execução medido seja o verdadeiro tempo de execução no pior caso. Isso porque o *WCET* pode ocorrer com pouca frequência, e as condições para que ele aconteça são normalmente desconhecidas.

Existe um conjunto de métodos de análise *WCET* que utilizam métodos estatísticos para fornecer estimativas de *WCET* que serão excedidas apenas com uma probabilidade máxima que é previsível. Esses métodos são baseados no ramo da estatística chamado Teoria dos Valores Extremos (TVE).

Uma estimativa do tempo de execução de uma tarefa no pior caso pode ser obtida a um determinado nível de confiança estatística, por meio do uso de medição para obter dados e da TVE para generalizar os processos que produzem essas medições. A previsão de um evento, ou a estimativa de um valor particular, pode ser feita usando provas obtidas por meio de medição. A TVE é um ramo da estatística que se baseia na modelagem do maior valor de uma amostra.

O objetivo da TVE é analisar valores extremos observados, e prever possíveis valores ainda mais extremos, inferindo sobre eventos cujas probabilidades são menores do que a probabilidade de qualquer evento observado anteriormente.

A principal dificuldade é que há uma exigência de generalizar o comportamento além do maior valor visto no conjunto de dados. Sem o uso de alguma técnica que pressupõe algum grau de comportamento generalizado, a melhor estimativa do *WCET* que pode ser feita é utilizar o maior valor observado, e ignorar todos os pontos de dados de valor menor. No entanto, o maior valor de dados obtido pode ser uma estimativa otimista do *WCET*. Em geral, assume-se que o maior valor observado terá uma chance pequena e desconhecida de ser o pior caso real.

## 2. Objetivo

Empregar o método de medições para estimar o *WCET* de tarefas que executam em sistemas de tempo real críticos. Será usado como estudo de caso um sistema operacional compatível com ARINC 653, a principal especificação de sistema operacional para sistemas aviônicos, já implementado sobre uma plataforma BeagleBone anteriormente. Eventualmente também poderá ser usada uma solução do tipo executivo cíclico em uma plataforma de hardware mais simples.

O objetivo geral deste projeto de mestrado é a avaliação de métodos e técnicas para estimar o tempo de execução no pior caso, em aplicações de tempo real. Busca-se métodos e técnicas estatísticas que sejam estruturados de tal forma a permitir lidar com arquiteturas de *hardware* e protocolos de comunicação modernos e complexos, de forma a obter estimativas mais confiáveis.

Deseja-se que os novos métodos e técnicas a serem propostos possibilitem obter estimativas de confiabilidade para os requisitos temporais e, conseqüentemente, garantir a segurança, a previsibilidade e a robustez do sistema, equilibrando esforços entre confiabilidade e custo. Ou seja, reduzir o custo testando o mínimo possível e garantir a confiabilidade maximizando a confiança de que os requisitos temporais são cumpridos.

### 3. Lista de Atividades

- (a) Estudar os conceitos básicos dos sistemas de tempo real.
- (b) Estudar a determinação do *WCET* através de medição.
- (c) Estudar os conceitos básicos dos sistemas operacionais ARINC 653.
- (d) Implementar uma aplicação exemplo no ARINC 653 disponível em BeagleBone.
- (e) Estudar o emprego de técnicas estatísticas e da Teoria dos Valores Extremos (TVE) para estimar o tempo de execução das tarefas no pior caso.
- (f) Montar um cenário de testes onde uma aplicação alvo será analisada, a fim de validar os métodos estatísticos.
- (g) Redigir artigos para publicação em congressos e/ou revistas.
- (h) Redigir a dissertação.

### 4. Bibliografia Parcial

- [1] R. I. Davis and A. Burns, A survey of hard real-time scheduling algorithms and schedulability analysis techniques for multiprocessor systems, *Systems Research*, 2009.
- [2] G. Buttazzo, *Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications*. Springer, 2 ed., 2005.
- [3] J. W. S. Liu, *Real-Time Systems*. Prentice Hall, 1 ed., 2000.
- [4] D. B. de Oliveira, R. S. de Oliveira, Timing Analysis of the PREEMPT RT Linux Kernel, *Software Practice and Experience*, Volume 46, Issue 6, pages 789–819, June 2016.
- [5] N. C. Audsley, A. Burns, R. I. Davis, K. W. Tindell, A. J. Wellings, Fixed priority pre-emptive scheduling: An historical perspective, *Real-Time Systems*, March 1995, Volume 8, Issue 2–3, pp 173–198.
- [6] R. I. Davis, A. Zabus, A. Burns, *IEEE Transactions on Computers*, Efficient Exact Schedulability Tests for Fixed Priority Real-Time Systems Volume 57, Issue 9, Sept. 2008.
- [7] R. S. de Oliveira. *Fundamentos dos Sistemas de Tempo Real*. Edição do autor, 2018.
- [8] R. Wilhelm, J. Engblom, A. Ermedahl, N. Holsti, S. Thesing, D. Whalley, G. Bernat, C. Ferdinand, R. Heckmann, T. Mitra, F. Mueller, I. Puaut, P. Puschner, J. Staschulat, Per Stenstrom. The worst-case execution-time problem - overview of methods and survey of tools. *ACM Trans. Embed. Comput. Syst.*, 7(3), 1-36, May 2008.
- [9] R. Wilhelm, T. Mitra, F. Mueller, I. Puaut, P. Puschner, J. Staschulat, P. Stenstrom, J. Engblom, A. Ermedahl, N. Holsti, S. Thesing, D. Whalley, G. Bernat, C. Ferdinand, and R. Heckmann. The Worst-Case Execution-Time Problem - Overview of Methods and Survey of Tools. *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 7, pp. 36:1–36:53, 2008.
- [10] R. I. Davis and L. Cucu-Grosjean, A Survey of Probabilistic Timing Analysis Techniques for Real-Time Systems, *Leibniz Trans. Embed. Syst.*, vol. 6, pp. 03:1-03:60, 2019.
- [11] R. I. Davis and L. Cucu-Grosjean, A Survey of Probabilistic Schedulability Analysis Techniques for Real-Time Systems, *Leibniz Trans. Embed. Syst.*, pp. 1–53, 2019.