

# Aplicação de SPARK no Desenvolvimento de Software Crítico

*Proposta de Mestrado*

Orientador: Simão Melo de Sousa

## 1 Contexto

Esta dissertação é para ser realizada em colaboração protocolada com a empresa Critical Software.

A garantia de que um software a executar num sistema crítico é uma tarefa não trivial que se torna cada vez mais necessária com a introdução de mais software em sistemas críticos. Geralmente a prova de que o software “está bem feito” é realizada por um conjunto de medidas e processos aquando o seu desenvolvimento e manutenção. No entanto com a evolução tecnológica que temos vindo a ter, e sendo tendência a evolução continuar a ritmos ainda maiores, é perceptível que os mais diversos sistemas serão cada vez maiores e mais complexos. Uma possível, e facilmente enumerada, forma de mitigar esse acréscimo de complexidade será a utilização de mais recursos (humanos e materiais) e mais tempo de desenvolvimento. No entanto, é também perceptível que a evolução está a acontecer a ritmos demasiado rápidos pelo que colocar mais pessoas ou estender os períodos de desenvolvimento não será a forma mais eficiente de endereçar tamanha evolução. Há nos dias de hoje uma preocupação de quem faz sistemas críticos que os mesmos sejam bem feitos logo durante a fase de desenho, vulgo “correct by design”. Para tal usam-se as mais diversas técnicas, desde a especificação baseada em modelos com validação dos modelos até a especificação matemática dos sistemas de modo a poderem ser provadas as premissas e propriedades desse mesmo modelo. Numa fase intermédia existe outro conjunto de técnicas que permitem garantir que alguns dos passos do desenvolvimento estão corretos por construção.

## 2 Objectivos

O objetivo deste projeto é fazer um estudo do uso de técnicas de anotação baseadas na tecnologia SPARK para validar que o fluxo de informação no software crítico é feito de acordo com a especificação. Além disso, com este tipo de anotações é possível garantir que o software que está a ser implementado cumpre com aquilo que é suposto ser feito. Sendo uma tecnologia usada apenas no desenvolvimento de sistemas críticos é expectável que haja uma boa dose de investigação operacional durante a dissertação de mestrado de modo a permitir obter resultados satisfatórios. Outro dos objetivos a endereçar no âmbito da dissertação é

a avaliação de ferramentas que possam ajudar no processo de desenvolvimento, ou em caso de necessidade na elaboração de um protótipo de ferramenta que permita obter os resultados expectáveis das análises de data flow e control flow.

### 3 Plano de Trabalho

As principais atividades a desenvolver no âmbito deste projeto são:

- T1 – Estudo do estado da arte no que diz respeito às técnicas baseadas em anotações, com particular ênfase na metodologia SPARK;
- T2 – Avaliar como se pode anotar os diversos fluxos de informação, as estruturas de dados e as declarações condicionais de modo a permitir obter um guia de utilização para as anotações SPARK.
- T3 – Identificar ferramentas e desenvolver um protótipo para utilização na verificação das regras/anotações identificadas na tarefa anterior.
- T4 – Avaliação e análise formal dos resultados obtidos pela análise do contrato SPARK implementado num caso de estudo a ser identificado durante a dissertação de mestrado.
- T5 – Produção do Relatório de Dissertação e de duas apresentações anexas, uma para a avaliação académica e outra, mais técnica, para uma apresentação pública na CRITICAL Software.

As tarefas aqui enumeradas poderão ser alteradas/complementadas se assim se entender durante a execução deste projeto sendo obrigatório nesse caso haver acordo entre o aluno, o orientador académico e o orientador industrial.

### 4 Contacts

Simão Melo de Sousa (desousa@di.ubi.pt)