Nos últimos anos, houve um grande avanço na indústria de semicondutores, o que possibilitou um aumento exponencial no desempenho dos microprocessadores. Esse aumento foi obtido graças à diminuição do tamanho dos transistores e da tensão com a qual eles trabalham. Entretanto, essas mudanças também resultaram na diminuição da confiabilidade dos transistores, deixando-os mais vulneráveis às falhas causadas devido à interferência da radiação. Duas das principais falhas que podem ocorrer quando um único íon colide no circuito são conhecidas como *Single Effect Upset* (SEU), quando provoca a alteração do valor armazenado em uma célula de memória, e como *Single Effect Transient* (SET), quando induz um sinal transiente na lógica combinacional do circuito, e ambas podem provocar erros tanto no fluxo de controle como no de dados do microprocessador. Portanto, aplicações de alta confiança, como espaciais ou aviônicas, necessitam de técnicas de tolerância a falhas que possam evitar ou recuperar o sistema após a ocorrência de um erro, sendo elas baseadas em redundância de software ou de hardware, ou em soluções híbridas. As técnicas baseadas em software proporcionam uma alta flexibilidade, além de um baixo tempo e custo de desenvolvimento, já que o hardware não precisa ser modificado. Contudo, costumam resultar em um considerável aumento no tamanho do código e no tempo de execução.

O presente trabalho, desenvolvido junto a uma tese de doutorado do PPGC, apresenta uma nova técnica híbrida para detectar falhas no fluxo de controle, baseada na implementação de um módulo de hardware não intrusivo, o qual controla os dados trocados entre o microprocessador e a memória, e em redundância de software. Usando um microprocessador MIPS e uma ferramenta que automaticamente protege códigos binários, foi realizada uma série de injeções de SEU e SET em todas áreas do MIPS, visando analisar a eficiência da nova técnica. Resultados mostram uma alta taxa de detecção com uma pequena perda de desempenho e aumento de ocupação.