Desesenvolvimento de Sistemas Instrumentados de Segurança na indústria do petróleo e gás utilizando métodos de teste e verificação formal

Orientador: **Prof. Max Hering de Queiroz**
Co-orientador: **Dr. Rodrigo Saad**
Área: Automação e Sistemas
Local de Desenvolvimento: DAS
Início: 08/2019
Previsão de Término: 02/2021

Objetivos:

O objetivo deste projeto de pesquisa é investigar a aplicabilidade de métodos que permitam garantir a integridade de sistemas instrumentados de segurança, tipicamente encontrados na indústria de petróleo e gás, em especial em unidades de produção *offshore*, buscando a operação segura e em conformidade com as especificações de funcionamento desses sistemas. Nesse sentido, pretende-se avaliar aplicação de métodos de *model-checking*, teste automático e *runtime verification* ao longo do ciclo de desenvolvimento do SIS de um processo real, qual seja, a Unidade de Experimentação em Escoamento Multifásico do DAS-UFSC.

Justificativa:

Sistemas críticos são sistemas geralmente encarregados de atividades de controle que requerem alto grau de confiabilidade, tendo em vista que falhas em tais sistemas podem levar a danos sérios de equipamentos de custo elevado e até em perdas de vidas humanas. A necessidade de atender os requisitos rigorosos deste tipo de sistemas exige que os projetos os levam em conta e que as implementações sejam previamente validadas. No caso da indústria de petróleo e gás, sistemas instrumentados de segurança são utilizados para garantir a segurança operacional de instalações industriais. Exemplos típicos são: Sistema de parada de emergência (*ESD-Emergency shutdown*); Sistema de parada de segurança (*Safety shutdown*); Sistema de intertravamento de segurança; Sistema de fogo e gás.

Os sistemas de controle lógico, sequenciamento e intertravamento de segurança se enquadram naturalmente na classe de Sistemas a Eventos Discretos (SED). Estes sistemas são caracterizados por um espaço de estados discreto de valores lógicos cuja dinâmica é dirigida pela ocorrência de eventos e podem ser representados por modelos formais. Na prática esses sistemas são geralmente implementados em CLPs adotando as linguagens das normas IEC 61131-3 e IEC 61499 e seguindo metodologias de projetos específicas do domínio da aplicação. No entanto, apesar da complexidade e da criticidade desses problemas, observa-se a pouca utilização de métodos formais na prática usual do projetista, seja na síntese de novos programas escritos nestas linguagens como na metodologia para validação de programas existentes ("legacy programs") ou novos, que garantam as boas propriedades da lógica de controle implementada.

No âmbito do Grupo de Pesquisa em Sistemas a Eventos Discretos e Híbridos (GSEDHI) do DAS, pesquisas recentes têm abordado tanto o uso de teste automático [1][2] como de verificação formal [3][4] para validação de programas de CLP, com foco no desenvolvimento de uma metodologia para validação da integridade de especificações de segurança para sistemas instrumentados de segurança de plataformas *offshore* ao longo de todo o ciclo de vida desses sistemas. Em [1][2], utiliza-se uma abordagem de testes do tipo caixa-preta em que os casos de teste são gerados a partir das relações entre entradas e saídas definidas pela especificação conforme padrão de Matriz de Causa e Efeito (MCE) definido pela I-ET-3000.00-1200-800-PGT-006, sem necessidade de se considerar a estrutura interna do programa de CLP. Casos de teste são derivados da MCE usando o método de grafo de causa e efeito e tabela de decisão de entrada limitada para cobertura eficiente de falhas. Em paralelo, Redes de Petri são usadas como oráculos que observam falhas perigosas ou seguras na execução do teste, sendo modularmente geradas a partir das especificações de segurança na MCE. Foi concebida uma ferramenta automática que permite editar a MCE, gerar casos de teste e oráculos, executar os casos de teste em um simulador de PLC, diagnosticar falhas a partir dos oráculos e apresentar os resultados. Um protótipo de ferramenta de teste automático foi desenvolvido e testado com sucesso para validação das especificações de segurança de uma plataforma offshore real.

Em [3][4] apresenta-se um método automatizável para verificação formal de programas de CLP em que as especificações de segurança de MCE são sistematicamente traduzidas em fórmulas LTL e o programa de CLP em diagrama Ladder é traduzido para um modelo formal para realização de *model-checking* através da cadeia de verificação TINA/SELT. Apresenta-se um método baseado em cone de influência para reduzir a complexidade dos modelos formais para SIS reais. Os contraexemplos resultantes são convertidos em diagramas de sinal ou em comandos para o simulador do CLP, que facilitam a interpretação das falhas identificadas. O método foi aplicado para verificação de um caso ilustrativo e do código do SIS de uma plataforma de petróleo *offshore* real.

Metodologia:

A presente pesquisa de mestrado tem como objetivo avaliar a viabilidade da aplicação desses métodos formais ao longo de todo o desenvolvimento e implantação de um SIS real. Diversos métodos formais serão analisados no contexto de um estudo de caso da planta do Laboratório para Experimentação em Escoamento Multifásico (LEEM) do DAS da UFSC, que foi projetado para produzir escoamento multifásico com proporções controladas de água, óleo e gás, além de permitir desenvolvimentos de instrumentação e técnicas de controle (Figura 1).

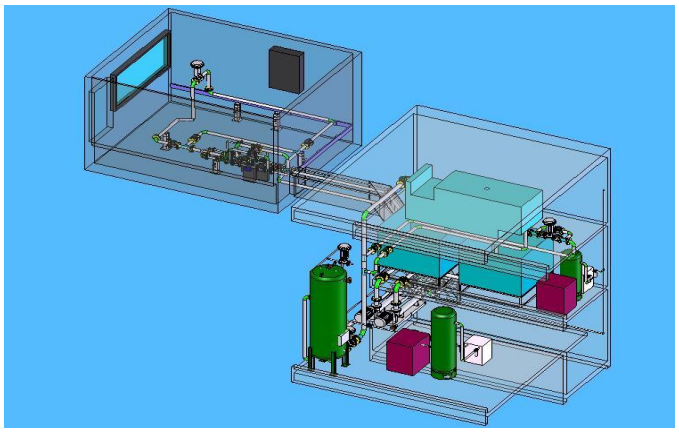

Figura 1: Planta do Laboratório para Experimentação em Escoamento Multifásico (LEEM)

Referências:

[1] T. J. Prati, J.M. Farines, M.H. de Queiroz *Automatic test of safety specifications for PLC programs in the Oil and Gas Industry* In: Proc. of the 2nd IFAC Workshop on Automatic Control in Offshore Oil and Gas Production. , 2015, Florianópolis. p.27 – 32

[2] H. W. Veiga, M.H. Queiroz, J.M. Farines, M. L. Lima. *Automatic Conformance Testing of Safety Instrumented Systems for Offshore Oil Platforms.* Lecture Notes in Computer Science. 1ed.: Springer International Publishing, 2017, v. , p. 51-65.

[3] Souza, M.F., Farines, J.M. and Queiroz, M.H., *'Modelagem e verificação de programas em Diagrama Ladder para Controladores Lógicos Programáveis'*. XVIII Congresso Brasileiro de Automática - CBA 2010, Bonito-MS, 2010.

[4] Reis, L. P. E. ; Queiroz, M. H. ; Farines, J.M. ; Lima, M. L. ; Campos, M. C. M. M. . *Verificação formal de Sistemas Instrumentados de Segurança na indústria de petróleo e gás natural.* In: Congresso Brasileiro de Automática, 2018, João Pessoa. Anais do XXII Congresso Brasileiro de Automática, 2018.