Proposta de Tema de Mestrado:
Aplicação de métodos de verificação formal ao projeto de programas de CLP na indústria de petróleo e gás

Orientador: Max Hering de Queiroz
Co-Orientador: Jean-Marie Farines

28 de junho de 2016

1 Objetivo

Esta proposta de pesquisa se origina no contexto de um projeto de pesquisa e desenvolvimento com a Petrobras intitulado "validação de sistemas de controle e automação na indústria do petróleo e gás utilizando métodos de teste, verificação e síntese de programas", que visa a operação segura e em conformidade com as especificações de funcionamento das unidades de produção *off-shore*. Especificamente neste trabalho de mestrado, pretende-se investigar as vantagens e limitações do uso dos métodos de verificação formal para o projeto de programas de controladores lógico-programáveis (CLP) neste domínio de aplicações e propor uma forma de incorporar esses métodos à atual metodologia de desenvolvimento de sistemas adotada pela Petrobras. Em pesquisas anteriores do grupo, desenvolveu-se um conjunto de ferramentas que compõem uma cadeia de verificação formal de programas de CLP implementados na linguagem *Ladder Diagram*, baseada em métodos de engenharia dirigida a modelos. Neste mestrado pretende-se estender essas ferramentas para as linguagens de especificação usadas pela Petrobras (Diagramas Lógicos, por exemplo) e ilustrar a metodologia proposta através de um estudo de caso inspirado em problemas reais de automação dos processos encontrados em plataformas de produção, em especial aquelas encontradas em plataformas *off-shore*.

2 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, danos ambientais e até em perdas de vidas humanas. A necessidade de atender os requisitos rigorosos deste tipo de sistemas exige que os projetos os levem em conta e que as implementações sejam previamente validadas. No caso da indústria de petróleo e gás, sistemas instrumentados de segurança são conjuntos de sensores, dispositivos lógicos e atuadores utilizados para garantir a segurança operacional de instalações industriais. Exemplos típicos são: Sistema de parada de emergência (Emergency shutdown); Sistema de parada de segurança (Safety shutdown); Sistema de intertravamento de segurança; Sistema de fogo e gás. A complexidade e criticidade de determinados sistemas automatizados como aqueles encontrados na indústria do petróleo gera a necessidade de se garantir que a lógica sendo utilizada nos controladores lógico-programáveis

(CLPs) e sua integração com os dispositivos de medição e atuação atende as especificações do sistema instrumentado de segurança.

Para fins de modelagem e análise, 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 industrial, 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.

3 Descrição do trabalho de mestrado

Neste trabalho de mestrado pretende-se realizar uma pesquisa exploratória sobre o uso de metodologias formais para modelar e verificar problemas reais de automação dos processos encontrados na indústria de petróleo e gás, baseada na modelagem e verificação formal de projetos de aplicações descritas nas linguagens de programação dos CLPs do padrão IEC 61131-3 [CLP, 2001]. A metodologia de verificação deve ser adaptada ao uso por engenheiros e projetistas desta indústria, para desenvolver a lógica de CLPs a partir das linguagens adotadas pela Petrobras para especificação de programas de CLP, em particular o Diagrama lógico, e permitir a translação destas em linguagens formais de descrição de comportamento (autômato, rede de Petri, sistema de transição temporizado). Por outro lado, as propriedades a serem verificadas tiram sua origem das especificações desejadas e representadas segundo a prática do usuário de cada indústria (como por exemplo, matrizes de causa-efeito). A metodologia proposta deve permitir a fácil transformação destas representações em expressões de lógica temporal que viabilizam a verificação de propriedades, e a eventual correção de erros antes da fase de implementação, a partir da apresentação de contra-exemplos de forma compreensível aos engenheiros.

Uma versão preliminar de ambiente para a modelagem e verificação de programas de controladores lógico-programáveis, escritos com Diagrama Ladder e alguns Blocos de Função foi desenvolvida em trabalhos anteriores [de Souza, 2010] [de Souza et al., 2010] [Farines et al., 2011] e testado numa aplicação de controle de sistema pneumático. Este ambiente baseado em engenharia de modelos (MDE) foi construído a partir de um conjunto de ferramentas encadeadas que, para programas de CLP gerados a partir de um editor open-source de linguagens para CLPs, Beremiz [Tisserand et al., 2007], permite verificar as propriedades destes com a ajuda da ferramenta de análise e verificação TINA [1]. A cadeia de ferramentas deste ambiente inicia com o editor de linguagem Beremiz que gera um código XML a partir do programa do CLP escrito em Diagrama Ladder e que é transformado numa linguagem intermediária de verificação FIACRE [Berthomieu et al., 2008]. O resultado da composição deste programa do CLP em Fiacre e da representação da planta na mesma linguagem, por sua vez é compilada num Sistema de Transição Temporizado TTS que serve de linguagem de entrada para a ferramenta TINA. Além disso, a descrição das propriedades a serem verificadas deve ser traduzida em especificações em TTS ou em lógica temporal que podem ser utilizadas respectivamente nas ferramentas de verificação por equivalência ou por "model-checking"da

[1] www.laas.fr/tina

ferramenta TINA.

Atualmente, um trabalho de mestrado em desenvolvimento no PGEAS vem adaptando esta metodologia para a verificação de propriedades de programas de CLPs implementados em Diagrama Ladder para sistemas instrumentados de segurança da indústria do petróleo e gás. Em paralelo, tem-se pesquisando no grupo o uso de métodos de teste caixa-preta para CLPs [Prati et al., 2015]. Esses trabalhos estão focados no teste de programas após a sua implementação no CLP. Por outro lado, a presente proposta de mestrado pretende abordar a fase inicial do projeto de sistemas de controle e automação, em que os engenheiros da Petrobras especificam o programa de CLP através de diagramas lógicos. Para isso, a metodologia que vem sendo desenvolvida e as ferramentas existentes deverão ser adaptadas para as linguagens de especificação adotadas pela Petrobras, na perspectiva de uma aplicação a um problema real. A metodologia será testada e avaliada através da verificação por técnicas de "model-checking"de propriedades de sistemas de CLPs em aplicações reais de petróleo e gás.

4 Etapas e Cronograma de Atividades

4.1 Etapas

O cronograma de atividades deste trabalho de mestrado segue as seguintes etapas:

1. Pesquisa Bibliográfica sobre as linguagens da norma IEC 61131-3, os modelos (rede de Petri, FIACRE, Lógica temporal), os métodos de verificação (“Model-checking”, equivalências, “Runtime verification”) e as ferramentas correspondentes;

2. Estudo sobre a metodologia de desenvolvimento de programas de CLP da Petrobras, visando a introdução de métodos de verificação;

3. Extensão da ferramenta existente de verificação de programas de CLPs para as linguagens de especificação adotadas pela Petrobras;

4. Modelagem e verificação das especificações do sistema de controle de um caso real da indústria de petróleo e gás, com a nova ferramenta;

5. Análise dos resultados;

6. Redação da dissertação e defesa.

4.2 Cronograma de Atividades

Este trabalho seguirá o seguinte cronograma:

Ano	Mês	Etapas					
		1	2	3	4	5	6
2016	setembro	x					
	outubro	x	x				
	novembro		x				
	dezembro		x				
2017	janeiro		x	x			
	fevereiro			x			
	março			x			
	abril			x	x		
	maio			x	x		
	junho			x	x		
	julho				x	x	
	agosto				x	x	
	setembro					x	
	outubro					x	x
	novembro						x
	dezembro						x
2018	janeiro						x
	fevereiro						x

Referências

[CLP, 2001] (2001). *IEC61131-3: Programming Industrial Automation Systems.*

[Berthomieu et al., 2008] Berthomieu, B., Bodeveix, J.-P., Filali, M., Garavel, H., Lang, F., Peres, F., Saad, R., Stoecker, J., and Vernadat, F. (2008). The Syntax and Semantic of FIACRE. Technical report, LAAS-IRIT-INRIA.

[de Souza, 2010] de Souza, M. F. (2010). Modelagem e verificação de programas de clp escritos em diagrama ladder. Master's thesis, PPGEAS-UFSC.

[de Souza et al., 2010] de Souza, M. F., Farines, J. M., and de Queiroz, M. H. (2010). Modelagem e verificaï£¡ï£¡o de programas em diagrama ladder para controladores lï£¡gicos programï£¡veis. In SBA, editor, *Anais do XVIII Congresso Brasileiro de Automï£¡tica - CBA 2010*, Bonito (MS).

[Farines et al., 2011] Farines, J. M., de Queiroz, M. H., da Rocha, V. G., Carpes, A. M. M., Vernadat, F., and Crégut, X. (2011). A model-driven engineering approach to formal verification of plc programs. In *Emerging Technologies & Factory Automation (ETFA)*, pages 1–8. IEEE.

[Prati et al., 2015] Prati, T., Farines, J., and de Queirozi, M. (2015). Automatic test of safety specifications for plc programs in the oil and gas industry. In *2nd IFAC Workshop on Automatic Control in Offshore Oil and Gas Production*, pages 27 – 32. IFAC. Florianopolis - Brazil.

[Tisserand et al., 2007] Tisserand, E., Bessard, L., and Souza, M. (2007). An Open Source IEC 61131-3 Integrated Development Environment. In *Proceedings of IEEE International Conference on Industrial Informatics - INDIN*, Vienna. IEEE.