Modelagem e verificação de programas de CLP para sistemas de instrumentados de segurança na indústria de petróleo e gás

Proposta de Dissertação de Mestrado
Orientador: Max Hering de Queiroz
Co-Orientador: Jean-Marie Farines

1 Objetivo

Este trabalho visa modelar e verificar o sistema de automação de uma aplicação real ligada ao setor de petróleo e gás, a partir de um ambiente para a modelagem e verificação formal de programas de controladores lógico-programáveis (CLPs) [Int03]. Num primeiro tempo, a aplicação alvo será ao sistema instrumentado de segurança em implantação no Laboratório para Experimentação em Escoamento Multifásico (LEEM) do DAS, que foi projetado para produzir escoamento multifásico com proporções controladas de água, óleo e gás, a fim de permitir desenvolvimentos de instrumentação e técnicas de controle. Num segundo tempo deste trabalho, a metodologia será aplicada a problemas reais de automação dos processos encontrados em plataformas de produção, em especial aquelas encontradas em plataformas *offshore*.

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 (ESDEmergency 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 aplicações descritas nas linguagens de programação dos CLPs do padrão IEC 61131-3. A metodologia de verificação deve ser adaptada ao uso por engenheiros e projetistas desta indústria, para programar CLPs a partir das linguagens usuais da norma IEC 61131 e permitir a translação destas em linguagens formais de descrição de comportamento (autômato, rede de Petri, sistema de transição tempori-

zado). 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.

Uma versão preliminar de um ambiente para a modelagem e verificação de programas de controladores lógico-programáveis, escritos com Diagrama Ladder e alguns Blocos de Função foi desenvolvida num trabalho anterior [dS10] [dSFdQ10] [FdQdR+11] 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 [TBS07], 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 e que é transformado numa linguagem intermediária FIACRE [BBF+08]. 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. Entretanto, nesta versão, as propriedades a serem verificadas por "model checking"são o resultado da interpretação pelo projetista das especificações escritas na linguagem do usuário e são introduzidas manualmente no nível das lógicas temporais LTL e CTL. Uma proposta de metodologia geral para a verificação de propriedades de sistemas com CLPs foi também desenvolvida.

Neste trabalho, a metodologia que vem sendo utilizada e o ambiente existente deverão ser adaptados e testados para sistemas instrumentados de segurança na indústria do petróleo e gás, 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. Num primeiro tempo, testes e avaliações poderão ser realizados sobre o sistema instrumentado de segurança a ser implementado no Laboratório para Experimentação em Escoamento Multifásico (LEEM) do DAS da UFSC.

[1] www.laas.fr/tina

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) e as ferramentas correspondentes;
2. Modelagem e verificação do sistema de controle do LEEM, com a ferramenta existente;
3. Extensão da ferramenta de verificação de programas de CLPs existentes com a introdução de um gerador de formulas de lógica a partir das especificações do usuário;
4. Modelagem e verificação do sistema de controle de um caso real da indústria de petróleo e gás, com a nova ferramenta;
5. Discussão 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
2015	setembro	x					
	outubro	x	x				
	novembro		x				
	dezembro		x				
2016	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
2017	janeiro						x
	fevereiro						x

Referências

[BBF+08] B. Berthomieu, J-P Bodeveix, M. Filali, H. Garavel, F. Lang, F. Peres, R. Saad, J. Stoecker, and F. Vernadat. The Syntax and Semantic of FIACRE. Technical report, LAAS-IRIT-INRIA, 2008.

[dS10] M. F. de Souza. Modelagem e verificação de programas de clp escritos em diagrama ladder. Master's thesis, PPGEAS-UFSC, 2010.

[dSFdQ10] M. F. de Souza, J. M. Farines, and M. H. de Queiroz. Modelagem e verificação de programas em diagrama ladder para controladores lógicos programáveis. In SBA, editor, *Anais do XVIII Congresso Brasileiro de Automática - CBA 2010*, Bonito (MS), 2010.

[FdQdR+11] J. M. Farines, M. H. de Queiroz, V. G. da Rocha, A. M. M Carpes, F. Vernadat, and X. Crégut. A model-driven engineering approach to formal verification of plc programs. In *Emerging Technologies & Factory Automation (ETFA)*, pages 1–8. IEEE, 2011.

[Int03] International Electrotechnical Commission - IEC. *IEC 61131-5 - Programmable Controlers - Part 3: Programming Languages*, 2003.

[TBS07] E. Tisserand, L. Bessard, and M. Souza. An Open Source IEC 61131-3 Integrated Development Environment. In *Proceedings of IEEE International Conference on Industrial Informatics - INDIN*, Vienna, July 2007. IEEE.