Um Modelo de Controle Formal para o gerenciamento de riscos de processo em fábricas de *software*

Felipe Rafael Motta Cardoso[1], Strauss Cunha Carvalho[2], Danilo Douradinho[3], Denis Ávila Montini[4], Paulo Marcelo Tasinaffo[5], Adilson Marques da Cunha[6]

[1]Instituto Tecnológico de Aeronáutica (ITA)
Praça Marechal Eduardo Gomes, 50, Vila das Acácias
Caixa Postal 12228-901 – São José dos Campos – SP – Brasil

felipe.reeves@gmail.com, strauss.carvalho@serpro.gov.br, danilodf@gmail.com, denisavilamotini@yahoo.com.br, tasinafo@ita.br, cunha@ita.br

1. Introdução

As empresas dependem cada vez mais dos sistemas de informação e da *Internet* para realizarem seus negócios e não podem sofrer interrupções em suas operações. Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, a confiança de seus clientes e o relacionamento com sua rede de parceiros e fornecedores [1].

Um incidente pode impedir a organização de cumprir sua missão e de gerar valor para o acionista. Neste sentido, a segurança da informação passa a ter um conceito mais amplo, não apenas relacionada com a esfera da tecnologia e das ferramentas necessárias para proteger a informação, mas também como um dos pilares de suporte à estratégia de negócio para o tomador de decisão de uma corporação.

Desenvolver sistemas seguros requer a utilização de métodos, técnicas e ferramentas que propiciem definir requisitos livres de inferências humanas e cuja análise de risco de processo esteja presente em todo o ciclo de vida do *software*.

Este artigo apresenta o protótipo de um metamodelo que contempla as Áreas de Processo de risco do modelo de qualidade CMMi-DEV e que utiliza o formalismo da Rede de Petri para gerenciar risco de processo em uma linha de produção de *software*.

2. Contextualização e Protótipo de Modelo

Desde a década de 60, a complexidade essencial dos sistemas de *software* de computador aumenta, na medida em que as aplicações precisam lidar com um número crescente de requisitos [2] e variáveis críticas. Descrições ambíguas de requisitos elevam a complexidade acidental no gerenciamento de riscos para o processo de desenvolvimento de *software*. A construção de sistemas cujas informações sejam seguras (confidenciais, íntegras e disponíveis), requer a especificação de requisitos livres de ambigüidades.

Uma solução que pode auxiliar na administração da complexidade acidental é a utilização de um Sistema de Informação Gerencial (SIG) [3], com o objetivo de verificar se os pontos chave do projeto resolvem o problema proposto, utilizando uma abordagem formal. Em um contexto de controle da qualidade amparada por segurança no desenvolvimento de projetos de *software,* este artigo visa construir um Modelo de Controle Formal (MCF) [4] que seja capaz de verificar o comportamento do produto gerado, considerando sua especificação. Tal avaliação propicia inspecionar o sistema de informações do projeto, a fim de reduzir a dependência das inferências humanas.

Para tal, propõe-se a utilização da Modelagem de Redes de Petri. Esta modelagem propicia uma representação matemática, contendo mecanismos de análise. Dado um modelo formal de estados finitos de um sistema, torna-se assim possível verificar o comportamento do sistema devidamente especificado [5].

A Figura 1 apresenta a visão macro de um metamodelo para o gerenciamento de riscos de processo em fábricas de *software* [6]. A estrutura deste metamodelo encontra-se formalmente definida por uma Rede de Petri, contendo as áreas de processo de risco do CMMi-DEV. O metamodelo apresentado será utilizado em uma fábrica de *software,* como suporte a um Sistema de Informação Gerencial (SIG).

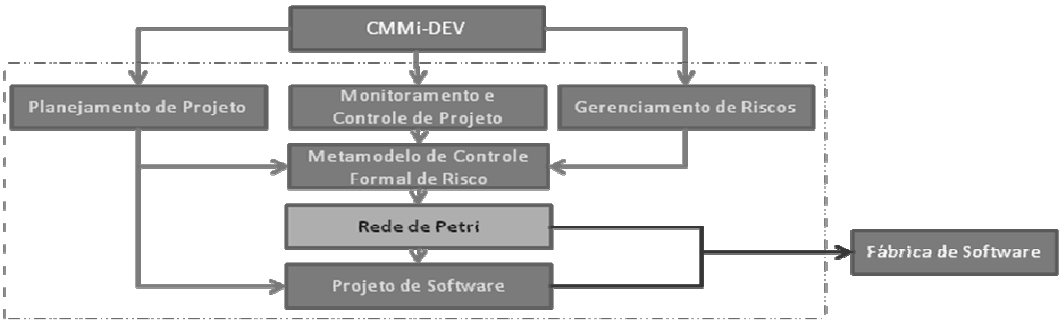

Figura 1. Visão macro de um metamodelo para o gerenciamento de riscos.

O monitoramento de riscos no processo de desenvolvimento de *software* envolve as três Áreas de Processo do CMMi [7]: de Planejamento de Projeto, que determina o impacto, a probabilidade, o período de ocorrência e a priorização dos riscos; de Monitoramento e Controle de Projeto; e de Gerencia de Risco, que identifica, *a priori* e de forma planejada, potenciais problemas para a administração de riscos, de acordo com as necessidades, ao longo do ciclo de vida de um Projeto, para mitigar impactos adversos.

3. Considerações Finais

O presente artigo relatou apenas alguns fragmentos de pesquisas em desenvolvimento pelo Grupo de Pesquisa em Engenharia de *Software* (GPES) da Divisão de Ciência da Computação do Instituto Tecnológico de Aeronáutica (ITA).

O protótipo de metamodelo para gerenciamento de riscos de processo visa propiciar a identificação, controle, análise e correção de problemas em uma linha produção de *software*, a fim de melhorar o monitoramento de riscos em processo para facilitar a tomada de decisão.

4. Referências

[1] Moreira, Nilton Stringasci. "Segurança Mínima: Uma Visão Corporativa de Segurança de Informações", Rio de Janeiro: Axcel Book, 2001.

[2] Pressmann, R. S. “Engenharia de Software”, 6ª edição p.752, McGraw Hill, NY, 2006.

[3] Laudon, Kennth C. & Laudon, Jane P. “Sistemas de Informação Gerenciais.” 7ª Edição. 2006.

[4] Moreira, Gabriel de Souza Pereira; Montini, Denis Ávila; Silva, Daniela América da; Cardoso, Felipe Rafael Motta; Dias, Luiz Alberto Vieira; Cunha, Adilson Marques da. *Design Patterns reuse for Real Time Embedded Software development.*. Las Vegas, Nevada, EUA 2009.

[5] MURATA, T. Petri net: *Properties, analysis and applications. Proceedings of the IEEE,* v. 77, p. 541-579, 1989.

[6] Montini, Denis Ávila, Modelo de indicadores de risco para o orçamento de componentes de software para célula de manufatura. .360p.Dissertação (Mestrado) em Engenharia de Produção – UNIP - (2005).

[7] CMMI, Version 1.2 - CMMI-DEV, V1.2, CMU/SEI-2006-TR-008 - ESC-TR- 006-008 - Improving processes for better products. August 2006.