IX ENFIR - Caxambu, MG (Outubro 1993)

UMA METODOLOGIA PARA CERTIFICAÇÃO DE SEGURANÇA DE CONTROLADORES DIGITAIS

Mário Mamoru Kotani (COPESP)
Antonio Souza Vieira Neto (IPEN/CNEN-SP)
Benício José de Souza (POLI-USP)
Wagner de Souza Borges (IME-USP)

RESUMO

Este artigo apresenta uma metodologia para certificação de segurança de controladores digitais com aplicação em instalações nucleares. Esta metodologia se aplica durante o desenvolvimento do projeto, e é baseada no princípio de refinamentos sucessivos. Devido a utilização de software a metodologia de certificação é orientada tanto para projeto quanto para o seu método de desenvolvimento.

INTRODUÇÃO

Controladores digitais críticos são produtos cuja utilização requer um alto nível de confiança na sua segurança. Para atingir os níveis de segurança adequados, uma fórmula já adotada em diversos países, consiste em implementar uma disciplina de avaliação independente, denominada certificação. A aplicação desta disciplina tem como objetivo a construção de um entendimento, técnicamente fundamentado, da propriedade de segurança, contribuindo assim para o aumento do nível de confiança nesta propriedade.

Neste trabalho, propõe-se um método de certificação para projetos de controladores digitais com funções de segurança em instalações nucleares. Este processo deve ser iniciado nas fases preliminares do desenvolvimento do projeto, para evitar o risco da equipe de certificação emitir um laudo considerando o produto insatisfatório do ponto de vista da segurança, em uma fase já adiantada do seu desenvolvimento. Nestas condições, os custos das modificações necessárias podem tornar-se proibitivos, inviabilizando a continuidade do projeto.

CERTIFICAÇÃO DE SEGURANÇA DE CONTROLADORES DIGITAIS CRÍTICOS

Na forma mais conhecida, certificação se refere a um procedimento independente de avaliação de um produto, com o objetivo de atestar o atendimento a requisitos, normas ou regulamentos específicos. O mesmo termo é aplicado também a processos independentes de avaliação de softwares, destinados a atestar a equivalência entre o serviço para ele especificado e o serviço por ele efetivamente produzido [1]. Portanto, um pouco de confusão é inevitável quando se introduz um procedimento independente de avaliação de um produto, com o objetivo de atestar propriedades específicas do mesmo, sob nome de certificação.

Em várias situações, um processo de certificação pode fundamentar-se na história de sucesso de produtos do mesmo tipo, com tecnologia, finalidade e condições de uso consagradas. Entretanto, no caso de controladores digitais com funções de segurança para aplicação em instalações nucleares, este tipo de abordagem não tem condições de ser utilizado devido, principalmente, às diferenças intrínsecas do software [2]. A certificação nestes casos deve derivar de um processo independente de análise de segurança.

METODOLOGIA PROPOSTA

O processo de certificação proposto neste trabalho é constituído por dois conjuntos de atividades implementadas por um grupo de especialistas, denominado equipe de certificação. No primeiro conjunto, a equipe de certificação estabelece as regras e os seus critérios de avaliação, e especifica os requisitos que, se atendidos, qualificam a utilização do produto como segura. No segundo conjunto de atividades, a equipe implementa as regras e critérios, e verifica o atendimento dos requisitos especificados.

Especificação dos Requisitos de Segurança. Os requisitos de segurança, estabelecidos pela equipe de certificação, devem ter como base normas e/ou recomendações de entidades credenciadas, especialmente da CNEN, da NRC, do IEEE, do IEC e da IAEA. Estas publicações apresentam, de uma modo geral, requisitos de caráter qualitativo e alguns casos abstraem o tipo de implementação utilizado no projeto.

Os requisitos de segurança devem ser refinados sucessivamente conforme as etapas de análise, tendo em vista a generalidade dos requisitos estabelecidos nas normas e/ou recomendações. Assim, é necessário que várias outras informações a respeito da instalação em que o controlador será aplicado sejam adicionadas para que a formulação dos requisitos possa ser obtida nos vários níveis de refinamento. Por exemplo, um requisito de "alta confiabilidade" deve ser traduzido em metas quantitativas de confiabilidade quando o nível de refinamento assim o exigir.

Especificação dos Requisitos da Metodologia de Desenvolvimento do Projeto. Os requisitos aplicáveis à metodologia de desenvolvimento estão diretamente ligados à garantia da qualidade e a experiência tem demonstrado que não é possível obter-se produtos de alta qualidade sem o emprego de um programa da garantia da qualidade adequado. Como exemplo particular pode-se mencionar o caso do software. Um dos requisitos de segurança aplicáveis ao software é que o mesmo seja de alta qualidade. Este requisito pode ser atendido com a utilização de uma metodologia de desenvolvimento bem estabelecida e de uma equipe de desenvolvimento qualificada. Portanto, os requisitos aplicáveis à metodologia de desenvolvimento do projeto deverão exigir:

a) a apresentação de um Programa da Garantia da Qualidade que contemple um programa específico que inclua do item objeto da certificação;

b) a elaboração de um conjunto consistente e completo de procedimentos relacionados com as sistemáticas de controle da qualidade, tais como: a de qualificação da equipe de projeto; a de verificação e validação e a de qualificação das ferramentas de apoio ao projeto.

Análise da Metodologia de Desenvolvimento. O objetivo desta análise parte do princípio de que um método de desenvolvimento de projeto adequado é fundamental não só para a qualidade do produto mas também para viabilizar sua avaliação no processo de certificação. Assim, esta análise deve seguir as seguintes etapas:

a) confrontação do método de desenvolvimento proposto pelo projetista com os requisitos estabelecidos pela equipe de certificação;

b) verificação da adequação de sua implementação.

Esta abordagem tenta garantir, portanto, que o produto será certificado somente se uma metodologia adequada tiver sido estabelecida e corretamente implementada.

Análise do Projeto. Para verificar os requisitos de segurança estabelecidos para o projeto são desenvolvidas atividades de análise para os componentes hardware e software levando-se em consideração as interações, dependências e formas de organização desses componentes. A análise deve ser conduzida de forma "top down" enfocando-se em um primeiro nível os aspectos da arquitetura do controlador, em um segundo nível os aspectos da arquitetura do hardware e do software separados, e finalmente as partes que compõem cada uma dessas arquiteturas.

Como os aspectos funcionais dos controladores estão ligados diretamente ao software, esta componente deve ser enfocada de maneira apropriada ao ser analisada. Assim, na análise de sua arquitetura este deverá ser enfocado como parte de um processo de controle, destacando-se a sua organização e sua interface com o suporte físico. Na sua análise funcional devem-se enfocar os algoritmos de controle implementados e as interfaces com o processo controlado.

A análise do projeto deve ser executada em fases, correspondendo aproximadamente às fases de desenvolvimento do projeto. Os produtos de cada fase de desenvolvimento são analisados aplicando-se os requisitos e critérios específicos estabelecidos pela equipe de certificação.

As Tabelas 1 e 2 apresentam o resumo das principais fases e métodos de análise.

RELACIONAMENTO COM O PROJETISTA E ORGANIZAÇÃO DA EQUIPE

Relacionamento com o Projetista. As atividades de certificação devem preferencialmente ser realizadas por equipes de organizações distintas das organizações projetistas. Entretanto, nos casos em que certificação for desenvolvida pela própria organização responsável pelo projeto é indispensável que os membros da equipe de certificação não sejam membros ou colaboradores da equipe de projeto e disponham de recursos adequados para o tipo de trabalho que irão executar.

Um requisito específico do processo de certificação proposto, é que as equipes de certificação e de desenvolvimento de projeto sejam independentes e autônomas. Independência, entretanto, não deve ser confundida com isolamento nem deve se converter em um fator de confronto entre as duas equipes. Estas duas equipes deverão produzir, com diversidade metodológica, evidências de que o produto é seguro, colaborando igualmente para a sua aceitação pelos agentes licenciadores. Assim, o ambiente para se estabelecer disciplinas inter-relacionadas de desenvolvimento e de certificação eficientes, deve proporcionar aos certificadores acesso irrestrito ao trabalho da equipe de projeto. É importante, também, que a equipe de desenvolvimento esteja consciente das necessidades da equipe de certificação e motivada para desenvolver um projeto passível de avaliação.

Outro argumento que destaca a importância da independência é fundamentado na diversidade metodológica de trabalho destas duas equipes. Enquanto a equipe de certificação investiga a existência de maneiras possíveis da utilização do produto resultar em um acidente, a equipe de projeto tem como objetivo produzir algo que faça aquilo que se deseja.

Organização, Capacitação e Atuação da Equipe de Certificação. O perfil básico dos membros da equipe de certificação inclui experiência e conhecimento específico em projeto, aplicação e análise do produto objeto da certificação bem como conhecimento dos requisitos de segurança aplicáveis.

A equipe de certificação é dividida em dois grupos. Um grupo legislador, ao qual cabe a definição das regras, critérios e requisitos para certificação, e um grupo executivo, ao qual cabe o desenvolvimento das atividades de análise propriamente ditas.

O grupo executivo é composto por analistas que desempenham as funções de presidente, relator, e inspetor.

O presidente age como elemento moderador e terá como principais atribuições:

a) obter e organizar a documentação necessária e suficiente para o processo de certificação;

b) convocar e moderar as reuniões de trabalho do grupo executivo;

c) elaborar planos estratégicos para o desenvolvimento do processo de certificação; e

d) indicar os analistas que desempenharão as funções de relator e inspetor.

O relator trabalha como coordenador executivo das atividades de certificação e suas principais atribuições são:

a) estudar o conjunto de documentos necessários e suficientes para o processo de certificação, e distribuir cópias deste material aos demais participantes do grupo;

b) elaborar o plano operacional para o desenvolvimento do processo de certificação;

c) elaborar as listas de verificação, com base nos requisitos de segurança, e distribuí-las aos inspetores; e

d) resumir os resultados das análises, obtidos pelos inspetores, e apresentar um relatório preliminar para discussão em reuniões de avaliação.

Os inspetores, com base nas listas de verificação, analisam a documentação de projeto, com o objetivo de identificar e descrever defeitos. A atuação dos inspetores deve, entretanto, ser independente, para que diferentes pontos de vista possam ser debatidos nas reuniões de avaliação.

A conclusão do processo de certificação se dá após o consenso do grupo executivo e será formalizado por um laudo contendo em anexo os principais documentos que lhe dão sustentação.

Ferramentas de Apoio à Certificação. A equipe de certificação deverá, preferencialmente, desenvolver suas próprias ferramentas computacionais que a auxiliem na execução de tarefas específicas de análise. Programas computacionais de análise, comercialmente disponíveis, deverão, de um modo geral, ser encarados com reserva devido a dificuldade se obter, nestes casos, a documentação completa da metodologia utilizada em seu desenvolvimento e os detalhes de sua implementação.

Deve ser enfatizado que, apesar das ferramentas computacionais fornecerem um apoio importante para a análise, um bom resultado do processo de certificação depende fundamentalmente da capacidade e da experiência do analista.

TABELA 1 Métodos e Ferramentas para a Análise dos Requisitos

Fase do Proj. / Métodos	PROJETO CONCEITUAL	PROJETO BASICO	PROJETO DETALHADO
REQUISITOS	- Requisitos gerais de segurança da arquitetura. - Classificação das Funções de controle.	- Requisitos específicos dos mecanismos de proteção.	- Métricas de estruturação do código. - Métricas de complexidade e de probabilidades de correção.
FERRAMENTAS	- Conhecimento do processo. - Base de projeto do processo. - Modelos de referência de arquiteturas. - Estudo da documentação.	- Modelos funcionais dos processos - Modelos dinâmicos das tarefas de controle. - Estudo da documentação. - Aplicação das teorias básicas.	- Documentação detalhada do processo. - Modelos estruturais das tarefas de controle. - Plano de testes. - Cálculo de Métricas. - Verificação formal.

TABELA 2 Método para a Análise da Arquitetura e Análise Funcional

Fase do Proj. / Análise	PROJETO CONCEITUAL	PROJETO BASICO	PROJETO DETALHADO
ARQUITETURA	- Descrição da arquitetura (hardware + software). - Classificação da arquitetura do sistema.	- Descrição da arquitetura do software. - Especificação das tarefas de controle. - Análise dos mecanismos de proteção interna.	- Códigos dos mecanismos de proteção. - Códigos das tarefas de controle. - Verificação da correção dos códigos dos mecanismos de proteção interna.
FUNCIONAL	- Lista e classificação das funções. - Análise de cobertura.	- Especificação funcional das tarefas de controle. - Análise das especificações das tarefas de controle.	- Código das tarefas de controle. - Verificação da correção dos códigos das tarefas de controle.

CONCLUSÃO

A certificação de segurança de um controlador exije uma metodologia que enfoque o processo de produção do controlador, principalmente quanto ao ítem software. Isto se deve ao fato das falhas do controlador terem origem em defeitos de projeto de difícil verificação uma vez implementado. Um acompanhamento dos estágios de produção pode propiciar meios de verificação em diversos estágios do produto, possibilitando um aumento da confiança em seu desempenho durante a operação.

Ainda não existe, a nível mundial, experiência consolidada de processos de certificação desenvolvidos em paralelo com o projeto [2]. Esta sistemática de certificação exige que o ciclo de vida do projeto seja claramente definido e que o controle da qualidade de seus produtos intermediários seja realizado de forma eficiente. Embora a certificação não consista propriamente da aplicação desse controle da qualidade, esta fica na dependência de seu sucesso.

A metodologia proposta neste trabalho encontra-se em fase de implementação em projetos em desenvolvimento na COPESP, de modo que não se tem ainda resultados suficientes que possam atestar sua eficácia. Pode-se, entretanto, constatar claramente que não se deve generalizar todos os detalhes do método proposto, considerando-se a grande quantidade de fatores que o afetam e que dependem do tipo e porte dos controladores, suas responsabilidades na segurança, o tipo de organização e experiência dos projetistas.

REFERÊNCIAS

[1] NEUMANN, B, Editor. **Software certification** Gatwick, UK., Elsevier Applied Science. 1989.

[2] REDMILL, F. J., Editor. **Dependability of critical computer systems.** vol.1, 2, 3. Crown House, Linton Road, Barking,.. Essex IG118JU, England. Elsevier Applied Science. 1988, 1989, 1990.

ABSTRACT

This paper presents a safety certification method for digital controlers with safety function in a nuclear facility. This method is supposed to be used simultaneously whith project development, and is based on the principle of successive refinements. Due to the existence of software components, the method is both oriented to project development methodology and design.