XI ENFIR - Poços de Caldas, MG, Brazil - 1997

"ANÁLISE DE CONFIABILIDADE E SEGURANÇA DE SISTEMAS DIGITAIS APLICADOS EM PROTEÇÃO DE REATORES NUCLEARES".

Pedro L. Benko* & José M. O. Neto**

*Centro Tecnológico da Marinha em São Paulo (CTMSP)
Av. Prof. Lineu Prestes, 2242 - Cidade Universitária, São Paulo-Brasil
CEP: 05508-900

**Instituto de Pesquisas Energéticas e Nucleares - (IPEN/CNEN-SP)
Caixa Postal: 11049, 05422-970, São Paulo- Brasil.

RESUMO

Propõe-se um método para desenvolvimento de Sistemas de Proteção Digitais tendo como base índices extraídos dos requisitos de Confiabilidade e Segurança da planta. Apresenta-se diretivas para avaliação desses dois fatores que são preponderantes na definição de arquiteturas para proteção e controle de plantas nucleares. São sugeridas técnicas e ferramentas para avaliação e modelagem de arquiteturas de *hardware* de proteção digitais computadorizadas. Para avaliação da qualidade do *software* sugere-se mecanismos de controle de projeto, especificação e procedimentos de verificação e validação (V&V).

I. INTRODUÇÃO

Os Sistemas de Proteção de Reatores Nucleares devem ser projetados segundo a ótica de equipamentos tipo falha segura. Portanto devem ter todos estados operativos e de falhas conhecidos e analisados, de modo que a ocorrência de um ou mais desses estados, não venham causar conseqüências indesejáveis para o homem e ao meio ambiente. O conceito de segurança está basicamente vinculado ao cumprimento desses objetivos, sobre os quais todo projeto deve ser conduzido.

O trabalho propõe que projetos dos sistemas eletrônicos de controle e proteção digitais, devem ter como ponto de partida, a especificação de índices de confiabilidade e segurança determinados a partir das necessidades específicas do arranjo da instalação.

A versatilidade, modularidade, compactação e facilidades de implementação de funções diversas, têm feito de sistemas digitais a tendência mundial no campo de controle e proteção de sistemas eletrônicos. Entretanto, as vantagens apresentadas podem ser contrabalançadas por uma redução na segurança da instalação se o sistema digital for concebido e implementado sem o emprego de métodos apropriados e específicos para o "*hardware*" e "*software*" que o compõem. Isto exige um complicado processo de certificação e qualificação [1].

II. CONVENCIONAIS X DIGITAIS

Para sistemas de proteção convencionais, as técnicas de análise de confiabilidade e segurança são bem conhecidas e o cumprimento de requisitos críticos de segurança são quantificáveis ou demonstrados por construção. Estes sistemas utilizam técnicas de topologias de circuitos "fail safe" e lógica de controle baseados em relés eletromecânicos. Possuem modos de falha conhecidos e estados de transição em caso de falha definidos.

Embora a tecnologia de computadores seja a vanguarda, a substituição de sistemas de proteção convencionais por sistemas informatizados encontra ainda grande resistência devido a falta de métodos consagrados para a quantificação dos parâmetros de confiabilidade e segurança.

Reconhecidamente, a tecnologia de computadores pode superar facilmente algumas limitações dos sistemas tradicionais, tais como: quantidade de informações processadas, níveis de automação, modularidade, precisão, calibração e monitoração, mas introduz novas incertezas.

O problema principal associado à certificação de sistemas digitais está na avaliação de qualidade do *software*. Segundo [2] "*Enquanto a quantificação da qualidade do software para grandes sistemas não puder*

ser feita de maneira probabilística, a qualidade de produção, verificação e validação independente e testes dinâmicos são uma alternativa qualitativa para demonstrar a adequação do propósito". Atualmente, esta é a prática adotada por todos os que desenvolvem sistemas para aplicações críticas.

O projeto de um *software* compreende a elaboração de um conjunto de especificações: o desenvolvimento do código; a aplicação de técnicas de verificação e validação; e o cumprimento de testes. O objetivo principal é obter um produto que , em primeiro lugar, tenha um conjunto de especificações adequadas à aplicação e, em segundo, um *software* que atenda plenamente a essas especificações.

O *software* para uma aplicação crítica pode ser complexo, de grande porte e, pelo fato de ainda hoje não se poder demonstrar de forma satisfatória a sua confiabilidade, deve-se assumir que ele possa conter erros.

A utilização de sistemas digitais para aplicações críticas tem sido aplicada em vários países. Na área nuclear a Agência Internacional de Energia Atômica (IAEA), a Framatome Francesa e a U.S. Nuclear Regulatory Commission estão investindo no desenvolvimento de diretrizes para projeto e verificação e validação (V&V) para licenciamento de *softwares* que atuem em sistemas críticos de plantas nucleares. [3]

III. DIRETIVAS PARA O DESENVOLVIMENTO DE SISTEMAS DE PROTEÇÃO DE REATORES

As seguintes fases de projeto, fazem parte das atividades relacionadas com a confiabilidade e segurança no desenvolvimento de Sistemas de Proteção de Reatores. A metodologia descrita é baseada nas referências [1],[2],[3],[4] [9] [10] [11] e na experiência adquirida em projeto de natureza semelhante desenvolvido no Brasil. O projeto de um sistema de proteção será dividido em três fases principais: Especificação de Sistema, Projeto Básico e Projeto de Detalhamento.

Especificação do Sistema. Nesta fase são definidas as funções e restrições do Sistema de Proteção em relação as necessidades da planta.

As atividades relacionadas à confiabilidade e segurança devem:

1. Utilizar os índices de confiabilidade, disponibilidade e segurança, obtidos na análise de segurança das instalações e considerando-se o sistema de proteção como um subsistema da planta. Podem ser utilizados como índices o MTTUF *(mean time to unsafe failure)* e a disponibilidade estacionária.
2. Determinar os requisitos de segurança e confiabilidade, específicos do projeto. Limitar a velocidade máxima de retirada de barras de controle, por exemplo, é um requisito que deve constar da especificação do sistema de proteção.
3. Especificar todos os tempos envolvidos tais como, tempo de missão, intervalos entre manutenções preventivas, tempos médios para correção de falhas etc.
4. Especificar todos os modos de operação e níveis de degradação aceitáveis.

Esses dados são imprescindíveis para o desenvolvimento das fases seguintes.

Projeto Básico. Esta fase define a arquitetura e os módulos básicos do sistema de proteção. Para atender os requisitos, índices e modos de operação definidos na fase de especificação, as seguintes atividades deverão ser cumpridas.

Definição da arquitetura. Para definição da arquitetura do sistema propõe-se:

- Avaliações de diferentes configurações de arquiteturas de sistema e plataformas de *hardware* e *software* visando determinar viabilidades, características e limitações.
- Definição da arquitetura de *hardware* do sistema de proteção com redundâncias se for o caso, e dos blocos funcionais que a compõem.
- Identificar as funções de segurança específicas para cada bloco funcional da arquitetura.
- Atribuir para cada modo de falha de cada bloco de *hardware* uma taxa de falha ou uma função de confiabilidade, constante ou dependente do tempo, ou do modo de operação. Esses parâmetros devem ser estabelecidos a partir de experiência anterior com módulos semelhantes, de dados fornecidos por normas ou referências confiáveis.

Modelagem do Arranjo da Arquitetura. Objetiva-se validar a arquitetura escolhida para o projeto através da modelagem da confiabilidade e segurança do arranjo.

Os dados a serem considerados para a determinação e análise do arranjo são os atribuídos aos módulos básicos que irão compor os blocos funcionais [4].

Dois tipos de modelagem são sugeridos, de acordo com a aplicação:

- Arranjos não reparáveis.
- Arranjos reparáveis, com taxas de manutenção definidas.

Deverão ser considerados os intervalos de verificações periódicas e índices de cobertura. Índice de cobertura é definido como a probabilidade de detecção de falhas de um sistema, subsistema ou módulo pelos mecanismos de testes ou procedimentos operacionais

O índice de segurança, MTTUF, deve ser comprovado na análise do arranjo de *hardware*. Os sinais trocados entre os blocos básicos, devem estar definidos, e estes sinais devem englobar variáveis de controle de processo, comunicação, alarmes e diagnósticos.

Uma aplicação de FMEA "análise de modos e efeitos de falhas", em nível de blocos básicos, pode ser

realizada considerando-se topologias de circuitos adequados em termos de segurança para a finalidade.

Os blocos básicos são usualmente identificados como porções não redundantes para análise de confiabilidade. Esses blocos devem ser unidades funcionais ou físicas bem definidas (memória, microcomputador, placa eletrônica, gaveta com cartões completa constituindo canal não redundante etc.).

Para os blocos caracterizados como não redundantes, qualquer modo de falha em cada um de seus componentes faz com que o bloco passe ao estado não operacional. Esta postura conservativa pode ser modificada quando existir uma intenção explícita de introdução de redundância em nível de componente ou placa.

Qualidade do *Software*. Os métodos tradicionais que avaliam a confiabilidade e a segurança de sistemas analógicos, reconhecidamente não são aplicáveis na avaliação da qualidade de sistemas digitais. O processo de engenharia de confiabilidade e segurança em sistemas computadorizados requer o cumprimento de atividades durante todo o seu ciclo de vida. Neste caso as mesmas devem ser estruturadas com o objetivo de obtenção de qualidade da especificação e qualidade do projeto. Por exemplo, as atividades que compreendem as fases iniciais do ciclo de vida do *software* [3] são:

- Plano de gerenciamento
- Plano de desenvolvimento
- Plano de instalação
- Plano de manutenção
- Plano de treinamento
- Plano de verificação e validação
- Especificação de requisitos de *software*
- Requisitos de análise de segurança.
- Requisitos de verificação e validação.

Fase de Detalhamento. A fase de detalhamento caracteriza-se pelo projeto de implementação do sistema de proteção.

Assim, todos os módulos básicos de *hardware* devem ser obtidos através de desenvolvimento próprio e ou aquisições no mercado. Todos os índices já foram atribuídos, as restrições conhecidas e o arranjo da arquitetura do sistema definido.

A implementação deve considerar: as configurações de circuitos; o arranjo físico dos componentes; a escolha dos componentes, arranjos de lay-out nas placas e nas gavetas, sendo que o projeto deve ser desenvolvido tendo-se em mente sempre as restrições de falha insegura.

Em nível macro, os projetistas devem ter um sentimento sobre o que estão cobrindo em termos de detecção de falhas e o que estão deixando de cobrir com relação às restrições de segurança, particular de cada módulo básico. Isto se faz necessário para determinação de índices de cobertura.

É necessário a figura de um gerente integrador, ou de uma ferramenta de integração entre os projetistas de *hardware* com projetistas de *software*. O elemento integrador deve agir de modo que ambos os projetistas tenham o conhecimento completo dos diagnósticos, índices de cobertura e tratamento de falhas[5], [6].

São necessárias reuniões periódicas de "revisão de projeto" com grupos externos e projetistas, para refinamento de idéias e identificação de problemas que possam ter passado despercebidos.

O mesmo procedimento se aplica quando forem adquiridas placas eletrônicas. O projeto deve ser conhecido, e os circuitos analisados pelo grupo responsável pela integração dos módulos básicos.

IV. AVALIAÇÃO DE CONFIABILIDADE DO *HARDWARE*.

Para se evitar erros sistemáticos de projeto, é necessária a criação de um grupo independente para análise de confiabilidade e segurança. Esse grupo terá acesso a todos os dados de projeto, e visará encontrar desvios que passaram despercebidos pelos projetistas e deverá também comprovar os valores metas de projeto.

Para análise de confiabilidade, o ponto de partida são os módulos básicos. A análise deverá ser efetuada da seguinte forma:

Obter taxas de falha para todos os componentes de cada módulo básico, utilizando-se fontes reconhecidas. Sugere-se como referência a norma MIL-HDBK 217 [11]. Em geral considera-se arranjo série de todos os componentes, onde a falha de um acarreta a indisponibilidade do módulo básico.

No caso de utilização da MIL HDBK 217 o método mais indicado para cada módulo de *hardware* é o cálculo dos índices de confiabilidade pelo método de análise de estressores,"*Stress Analysis*", que define de forma mais completa a taxa de falhas de cada componente, considerando a solicitação física a que o mesmo está sendo submetido na aplicação.

Calcula-se a seguir a taxa de falhas e o índice de confiabilidade de cada módulo básico obtendo-se os valores quantificados para o projeto.

Os índices determinados devem então substituir as taxas atribuídas para *hardware* na fase do projeto básico, e os índices globais do Sistema devem ser recalculados.

Caso os valores obtidos não atendam às especificações, serão necessários ajustes no projeto dos módulos ou da arquitetura.

A avaliação de confiabilidade do modelo da arquitetura, no caso de arranjo com reparo, é efetuada por *cadeias de Markov*. O modelo de transição de estados de falha deve ser ajustado de acordo com as taxas de falhas λ obtidas no calculo de confiabilidade de cada módulo e taxas de reparos μ atribuídas segundo dados do projeto. Estas taxas serão correspondentes a probabilidades de transição de um determinado estado

para outro no modelo. Os valores encontrados deverão atender a especificação.

Para arranjos sem reparo, a arquitetura deverá ser avaliada por combinações série e paralelo de funções confiabilidade dos blocos básicos.

V. AVALIAÇÃO DE SEGURANÇA DO *HARDWARE*

A análise de segurança de uma arquitetura de *hardware* deve ser iniciada sempre através da identificação dos eventos topo que causariam o estado inseguro para o sistema [5].

De posse dos requisitos básicos de segurança, deverão ser identificados os eventos primários de falhas que combinados resultariam no evento topo de uma condição não segura. O método propõe a realização de uma análise desta arquitetura por FTA "análise por árvore de falhas".

Este procedimento pode ser realizado tanto a nível de arquitetura quanto a nível de canal redundante.

Em nível de módulos básicos, quando se dispõe de dados de projeto, recomenda-se uma exaustiva análise de FMEA para detecção de falhas simples de componentes que causariam situações inseguras para o módulo básico. Estas falhas deverão ser classificadas conforme o seu grau de importância (monitoradas, detectáveis, não detectáveis e críticas). O objetivo é determinar a existência de falhas críticas e suas probabilidades de ocorrências. Recomenda-se também um FTA de falhas combinadas, para componentes e circuitos comuns dependentes entre si, ou que possuam dependência de função sobre eventos topos que causariam situações não seguras.

De posse dos dados de taxa de falha insegura deve-se calcular o MTTUF para o sistema considerando-se todas as redundâncias e votações através da modelagem de cadeias *Markov* para o diagrama de transição de estados operacionais do sistema. Considera-se as classes de falhas apontadas pelo FMEA, tempos médios de detecção através de diagnósticos, taxas de falhas, taxas de reparos, tempos de missão etc. A probabilidade de ocorrência do estado absorvedor caracteriza o grau de uma condição não segura.

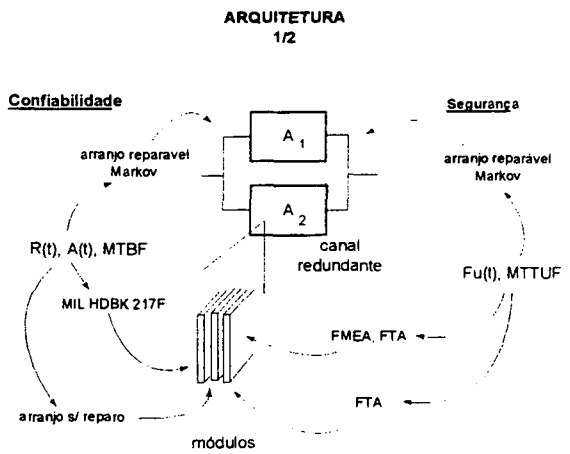
O valor obtido de MTTUF deve atender ao especificado no projeto de concepção.

É comum a utilização do conceito MTBUF (*Mean Time Between Unsafe Failure*), porém verifica-se que em sistemas de proteção de reatores este conceito não é adequado uma vez que a ocorrência de falha insegura pode resultar em um acidente onde o sistema e a planta não sobreviveriam. Logo o termo MTTUF expressa um índice de expectativa média de tempo para falhar, caracterizada por um estado sem volta, mais realista que o termo MTBUF.

VI. ILUSTRAÇÃO DO MÉTODO.

A figura abaixo ilustra o método proposto apresentando um esquema genérico para a avaliação da confiabilidade e segurança de uma arquitetura, com redundância 1 de 2, considerando cada canal redundante como um módulo básico, onde qualquer falha de componente coloca este módulo em falha.

Diagrama do método para análise de confiabilidade e segurança



VII. AVALIAÇÃO DA CONFIABILIDADE E SEGURANÇA DO *SOFTWARE*

Atualmente, não se dispõe de procedimentos ou mecanismos consagrados que possam mensurar níveis de qualidade e segurança de um *software* em nível de qualificação.

Um *software* não apresenta falhas se estiver atendendo uma especificação adequada. Partindo-se deste princípio, verifica-se que um meio de garantir a qualidade do *software* é o desenvolvimento criterioso do projeto durante todo o seu ciclo de vida [3] e um acompanhamento minucioso da operação do equipamento, durante o período de qualificação.

As técnicas orientadas ao objeto tem se mostrado como uma alternativa à técnica estruturada, apesar de serem consideradas mais trabalhosas e menos conhecidas para aplicação em sistemas de controle. Porém são mais fáceis de rastrear e corrigir devido ao encapsulamento de dados nos objetos.

A princípio, os seguintes itens devem ser considerados no desenvolvimento do *software*.

1) Projeto detalhado, documentado e acompanhado durante todas as fases de desenvolvimento.

2) Análise de segurança do código dos módulos de *software* relacionados com segurança e uma análise de interferência dos módulos não relacionados com segurança, a qual deve prever:

- Mapeamento dos requisitos nos módulos de *software* relacionando a especificação á implementação.

- Separação das partes relacionadas com segurança das não relacionadas.
- Inspeção das partes relacionadas à segurança segundo uma lista de verificação pré-estipulada. relativas ao fluxo de dados e ao fluxo de controle. segundo critérios funcionais e estruturais.
- Inspeção de partes não relacionadas com a segurança. segundo uma lista de verificações pré-estipulada. visando identificar interferências desses módulos sobre os módulos relacionados á segurança.
- Realização de *"Walk-Through"* segundo procedimento padronizado, das partes relacionadas mas identificadas como interferentes na inspeção.

Na fase de validação. instalação e operação. as principais atividades relacionadas à análise de confiabilidade e segurança são o acompanhamento de falhas de manutenção e o levantamento de erros de *software*[4].

Os dados coletados servirão para ajustes no índices de confiabilidade de *hardware* calculados e para qualificação do *software* por tempo de operação sem o aparecimento de erros.

Um aspecto importante é a qualidade de documentação gerada. Um dos processos para se avaliar a qualidade de um *software* é a qualidade de sua documentação de projeto. onde todos os requisitos podem ser verificados e todos os procedimentos validados. Porém qualidade não significa quantidade. pois conforme [7], importantes conclusões são retiradas do processo de licenciamento de uma planta CANDU em Ontario Hydro no Canadá. O autor expõe que *"A produção de massiva quantidade de documentação de software não deve tornar-se um fim em si próprio. Idealmente. a documentação deve ser axiomaticamente produzida como uma parte inerente do projeto e processo de verificação e deve ser precisa e clara o bastante para habilitar revisões efetivas por todos diferentes grupos de interesse no sistema"*. Com isso conclui-se que os documentos não devem ser criados porque simplesmente devem ser produzidos. e sim devem ser criados somente se forem relevantes para o projeto. e o devem ser de forma a clarear dúvidas e não confundi-las.

Quanto ao aspecto quantitativo. existem vários modelos de crescimento de confiabilidade disponíveis que se propõem a avaliar a confiabilidade de um *software* em várias fases de sua vida. Existem modelos matemáticos para as fases de: desenvolvimento, validação. vida operacional e manutenção. Temos até modelos em medidas de correção. Entretanto. em termos de qualificação. não bastam ao órgão licenciador. servem apenas como modelos experimentais que auxiliam no seu ciclo de vida e buscam solidificar-se como ferramenta de projeto durante as atividades de testes [3].

Convém salientar. que em sistemas críticos. o *hardware* computacional deve ser considerado durante o cumprimento de requisitos de segurança pelo *software*.

Duas fontes para balizar o desenvolvimento de *software* podem ser as normas IEC-880 de 1986 [9] e mais recentemente a IEEE 7-4.3.2 de 1993 [10].

VIII. CONCLUSÃO

Sistemas digitais são atrativos porque tem flexibilidade e facilidade de implementação de funções de controle, proteção e monitoração. Possuem também rapidez e precisão no processamento de sinais. permitindo o processamento de funções complexas em um tempo de reação curto e ergonomicamente aceitável. Além disso, o equipamento em operação não está sujeito a derivas e calibrações, minimizando tempos de manutenção e com isso reduzindo a incidência de erro humano. Porém, possuem sérias dificuldades de certificação junto aos órgãos licenciadores devido aos processos atuais de comprovação de confiabilidade e segurança relativos ao *software*.

Baseado nessas premissas o método proposto é apoiado basicamente em qualidade de projeto e documentação e estabelece que em sistemas de segurança o *software* não pode ser tratado de forma isolada em relação ao *hardware*. As ferramentas propostas para análise da arquitetura de *hardware* já são consagradas e constituem uma alternativa prática de avaliação durante o desenvolvimento de um Sistema de Proteção de Reator com vistas a segurança confiabilidade e qualificação. Verifica-se que os procedimentos de análise de segurança e confiabilidade para comprovação da integridade de *softwares* sugeridos e empregados atualmente. ainda não são consagrados e por isso geram dúvidas de sua efetividade junto a orgãos licenciadores. Como resultado ocorre um maior rigor de processos de certificação e consequentemente. atrasos. A experiência adquirida junto ao CTMSP e com os resultados de estudos realizados [12], mostram que o uso de sistemas digitais para aplicações críticas. é hoje uma tecnologia emergente que deve-se consolidar.

IX. BIBLIOGRAFIA

[1] Q.B. Chou. P. N. Acchione. R. J. Hohendorf. **Digital Technology in Nuclear Power Plants - White Knight or Black Hole?** - Ontario Hidro. 700 University Avenue - Toronto. Proceedings - Topical Meeting on Nuclear Plant Instrumentation. Control and Man-Machine Interface Technologies. April. 1993.

[2] Geoffrey Ives; **Digital Systems - Review of Safety Critical Applications** - Nuclear Engineering International - Instrumentation & Control. April 1994

[3] **Software Reliability and Safety in Nuclear Protection Reactor** - Lawrence Livermore National Laboratory; report prepared for "U.S. Nuclear Regulatory Commission". 1993.

[4] Francisco J. O. Dias, Marcio M. Coelho **Qualificação de equipamentos de segurança** - Depto de Engenharia de Computação e Sistemas Digitais - EPUSP, Quad-log Eletrônica Ltda - Apostila, 1989.

[5] S. Utena, T. Suzuki, H. Asano, H. Sakamoto. **Development of the BWR Safety Protection System with a new Digiital Control System** - International Symposium of Nuclear Power Plant Instrumentation and Control - Tokyo, Japan 1992.

[6] A.B. Keats - **Failsafe Design Criteria for Computer based Reactor Protection Systems** - Nuclear Energy, vol 19, Dec., Número 6, 423-428, 1980.

[7] James T. Keiper - **Application of Digital Control Systems in Nuclear Power Plants** - Nuclear Engineering Conference - volume 2 ASME, 1993.

[8] Henrique M. Paula and Michael W. Roberts, **Reliability Performance of Fault-Tolerant Digital Control Systems** - JBF Associates, Inc., Knoxville, TN 37932; Ronald E. Battle, OAK Ridge National Laboratory, OAK Ridge, TN 37831 - Plant/Operations Progress (Vol 10. No. 2). April, 1991

[9] IEC 880, **"Software for Computers in the Safety Systems of Nuclear Power Stations"**, 1986.

[10] IEEE 7-4.3.2-1993, **"Standard Criteria for Digital Computers in Safety of Nuclear Power Generations"**, 1993

[11] MIL - HDBK-217E, **"Reliability Prediction of Electronic Equipment"**, 1986 .

[12] Benko, Pedro Luiz, **"Um Estudo de Arquiteturas de Hardware Digital para aplicação em Sistemas de Proteção de reatores Nucleares - Métodos de Análise de Confiabilidade e Segurança"**. Dissertação de mestrado em conclusão, IPEN-1997.

ABSTRACT

A method for developing digital protection systems based upon reliability and safety requirements has been proposed. Directives for assessing such conditions are suggested. Techniques and the most common tools employed in hardware evaluation and modelling of such architectures have also been shown. In order to estimate the software quality, several mechanisms to control design, specification, and validation and verification (V&V) procedures are suggested.