Os desafios do licenciamento de sistemas digitais de instrumentação e controle em Usinas Nucleares

The challenges of licensing of digital instrmentation and control system in Nuclear Power plants

Tatiane Melo Vital†*, Richard Brandão Nogueira Vital†

Como citar esse artigo. Vital, TM; Vital, RBN. Os desafios do licenciamento de sistemas digitais de instrumentação e controle em Usinas Nucleares. Revista Teccen. 2019 Jan/Jun; 12 (1): 50-59.

Resumo

Os processos de obsolescência e desenvolvimento de novos projetos de usinas nucleares demandam por equipamentos/componentes de Instrumentação e Controle (I&C) com melhor desempenho atendendo a requisitos de segurança cada vez mais rígidos. Em função dessa demanda, a aplicação de sistemas digitais de I&C apresenta-se como uma boa solução tecnológica, mas precisa ser validada por processos específicos de licenciamento. Diante da importância do assunto e da demanda existente, este artigo apresenta algumas atividades que tem sido realizadas para atender aos requisitos e recomendações de diversos reguladores do setor nuclear. Dessa forma, são mostrados os pontos de maior questionamento regulador e experiências sobre o processo de licenciamento de sistemas digitais de I&C em diferentes culturas reguladoras.

Palavras-Chave: Usina Nuclear, Licenciamento, Instrumentação e Controle.

Abstract

Obsolescence process and new nuclear power plant designs demands instrumentation and control equipment and components with better performance and it shall attend stronger safety requirements. To attend this demand, the application of digital I&C appears like a good technologic solution but shall be validated by specific licensing processes. Due the importance and demand of this subject, this paper shows some activities that had been executed to attend requirements and recommendations of nuclear regulators. This work presents the highlights and experiences of digital I&C licensing in different regulator culture.

Keywords: Nuclear Power Plant, Licensing, Instrumentation and Control.

Introdução

A produção de energia elétrica através utilização do calor gerado em sucessivos processos de fissão pelos reatores nucleares de potência segue um rigoroso processo de licenciamento que tem como objetivo proteger as pessoas e o meio ambiente dos riscos relacionados à operação do reator (IAEA, 2016a). O processo de licenciamento de uma usina nuclear deve levar em consideração os riscos associados a cada fase, desde a definição do local até a etapa onde o controle regulador não se faz mais necessário. A Agência Internacional de Energia Atômica (IAEA) através do Guia Específico de Segurança SSG-12, distribui o tempo de vida de uma usina em sete estágios como pode ser observado na Figura 1 (IAEA, 2010).

O estágio de escolha de local para instalação de uma usina nuclear deve levar em consideração: os aspectos físicos do local (sismologia, meteorologia, geologia e hidrologia); densidade populacional; condições de acessibilidade; posicionamento de centros consumidores de energia e disponibilidade de malha de distribuição. Na fase de projeto é avaliado como os recursos tecnológicos disponíveis podem ser arranjados para atender aos requisitos reguladores existentes, de forma a evitar riscos durante uma operação normal ou em caso de acidentes. A fase de construção consiste na aplicação das melhores práticas disponíveis para se garantir as margens de segurança definidas durante o projeto e sua compatibilidade com o local escolhido

Afiliação dos autores: † Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – CEFET/RJ
‡ Universidade Federal do Rio de Janeiro - UFRJ

* Email para correspondência: tati.mv7@gmail.com

Recebido em: 23/03/19. Aceito em: 23/05/19.

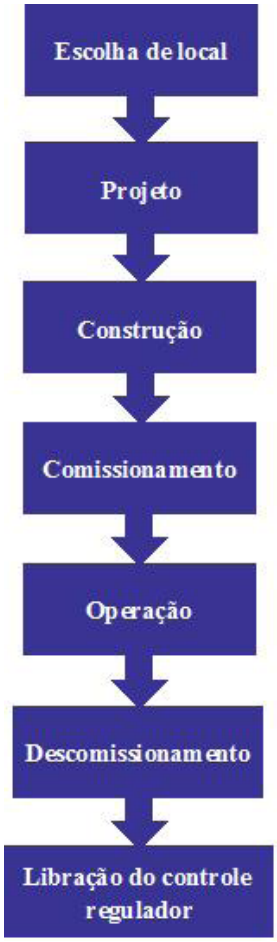

Figura 1. Etapas do licenciamento de uma instalação nuclear.

e, dependendo do modelo regulador do país, exige um Relatório Preliminar de Análise de Segurança (RPAS) com requisitos específicos. O Comissionamento de uma usina consiste na avaliação do comportamento dos sistemas que foram instalados e a adequação dos limites obtidos com os valores previamente analisados. Quando uma usina recebe a autorização de operação, a mesma deve operar conforme os limites e requisitos reguladores definidos no Relatório Final de Análise de Segurança (RFAS) (CNEN, 2002). Quando o tempo de operação de uma usina atinge o limite licenciado, inicializa-se um processo de descomissionamento para avaliar as condições das estruturas e componentes que poderão ser descartados ou, quando necessário, realizam-se processos de descontaminação e armazenamento de rejeitos radioativos. O empreendimento somente sairá do controle regulatório quando for comprovado que todos os riscos relacionados a radioatividade foram removidos da instalação.

Dentro do processo de licenciamento, os requisitos são constantemente revalidados através de Análises de Segurança, uma vez que um empreendimento desse tipo pode operar por mais de 40 anos (IAEA, 2012). Quando um sistema ou componente sofre degradação a ponto de interferir no desempenho operacional, uma substituição torna-se necessária para a continuidade da atividade comercial. Entretanto, muitos materiais passam por um processo de obsolescência, visto que em muitos casos as práticas comerciais e industriais passaram por processos de modernização, tornando difícil a aquisição de componentes antigos. Atualmente, a obsolescência tem se apresentado como um obstáculo, pois interfere diretamente nas atividades de manutenção (Rojo, Roy & Kelly, 2012). Para que uma usina continue a operar respeitando as condições de segurança licenciadas, diversos processos de modificação do projeto original podem ser implementados. O desenvolvimento de novos projetos de reatores também tem influenciado a busca por tecnologias mais baratas e seguras (Wahlström, 2007). Os guias SSR-2/1 IAEA (2016b) e

SSR-2/2 IAEA (2016c) da IAEA recomendam diversos requisitos que devem ser levados em consideração durante o desenvolvimento ou modificações de projeto de um reator nuclear. Esses requisitos apontam para importantes características e funções que os sistemas de segurança devem desempenhar durante uma operação normal ou em caso de acidentes.

Os projetos das usinas têm sido automatizados através de diversos sistemas de I&C, que visam aumentar a rapidez no controle das variáveis de processo e redução de falhas de origem humana. Os primeiros sistemas de I&C utilizados em reatores nucleares eram analógicos, mas devido aos efeitos de obsolescência, necessidade de redução dos custos e introdução de novos requisitos ou inovações tecnológicas, tem perdido espaço para os sistemas digitais (Wahlström, 2015).

Diante do contínuo aprimoramento dos processos de regulação e da eminente necessidade de inclusão de novas tecnologias nos projetos de usinas nucleares, os processos de análise de segurança precisam empregar metodologias mais robustas e eficientes. Portanto, esse trabalho apresenta algumas etapas do processo de licenciamento e dificuldades relacionadas ao licenciamento dos sistemas digitais de I&C, considerando experiências obtidas em diferentes modelos de regulação.

Requisitos para Sistemas de I&C

Os sistemas de I&C permitem que os operadores da planta monitorem o desempenho operacional, atuem sobre os sistemas ou identifiquem situações anormais, atendendo aos requisitos e limites de projeto (IAEA 2011). A Figura 2 ilustra a estrutura para aquisição de dados da planta, tratamento das variáveis monitoradas e atuação sobre sistemas de acordo com as margens licenciadas. No modelo apresentado, verificam-se duas estratégias de controle: a atuação manual, onde os operadores possuem uma interface homem-máquina que permite o controle operacional dos sistemas da usina e a atuação automática, onde comandos são gerados devido ao desvio de algum parâmetro ou compensações operacionais.

Nos sistemas de I&C analógicos, as informações obtidas por sensores de campo são processadas por circuitos baseados em relés ou analógicos. Nos sistemas digitais, os sinais de entrada ou saída dos módulos são processados por dispositivos lógicos reprogramáveis como as famílias FPGA (*Field-Programmable Gate Array*) e CPLD (*Complex Programmable Logic Device*) (Wyatt & Supler, 2017).

De acordo com a função desempenhada, os sistemas podem ser classificados como "importantes"

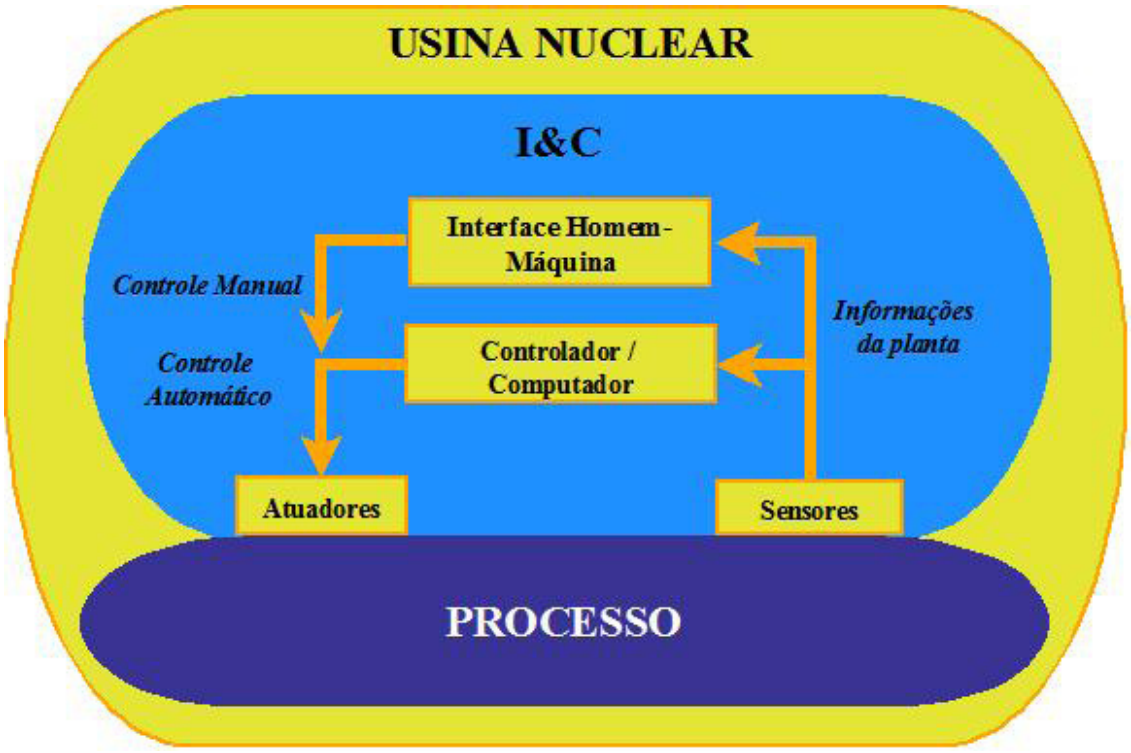

Figura 2. Interação entre blocos de um sistema de I & C e o processo controlado.

Revista Teccen. 2019 Jan/Jun.; 12 (1): 50-59

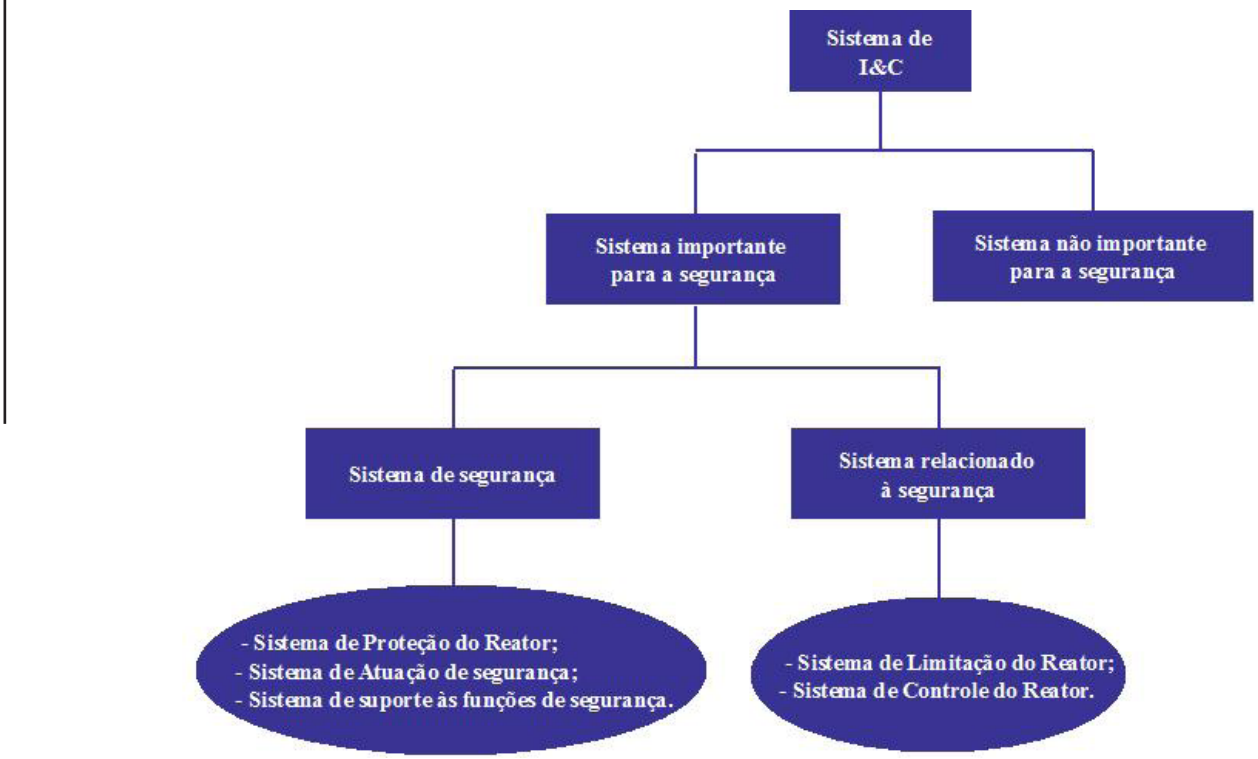

Figura 3. Classificação dos sistemas de I&C.

ou "não importantes" para a segurança. A Figura 3 mostra a classificação de alguns sistemas de acordo com as funções de segurança desempenhadas.

A classificação da importância de um sistema para a segurança de uma usina é calcada em três fatores [1]:

- Conseqüências que uma falha pode provocar em uma função de segurança;
- Freqüência de ocorrência do evento iniciador postulado para cada função demandada;
- Tempo após inicio do evento iniciador postulado ou período de execução da função.

Durante a fase de projeto de uma usina nuclear, o Guia SSR 2/1 IAEA (2016b) apresenta nove requisitos específicos para I & C, que são mostrados na Tabela 1.

Desafios do licenciamento dos sistemas digitais

Tomando como base os requisitos das diversas etapas da vida de uma usina nuclear, a IAEA listou os desafios de um processo de licenciamento de sistema digitais de I&C em 17 grupos, considerando as experiências já testadas por operadores, reguladores, projetistas e fornecedores (IAEA, 2012). Para mostrar os benefícios e desafios do processo de licenciamento são apresentados alguns exemplos de problemas encontrados mundialmente em diversos modelos de regulação.

Autodiagnostico dentro de uma plataforma digital de I&C

Uma das vantagens da aplicação da tecnologia digital é a possibilidade de se diagnosticar antecipadamente desvios operacionais ou falhas de componentes, através de: testes periódicos de integridade de memória, falha em lógica e condições dos dispositivos de entrada e saída (IAEA, 2012). Do ponto de vista dos projetistas e operadores, a inclusão dos autodiagnostico vislumbra reduzir o tempo gasto com testes periódicos, mas muitos reguladores estão relutantes quanto a esta substituição. Os questionamentos quanto a expansão do emprego das técnicas de autodiagnostico são direcionados à segurança dos sistemas, uma vez que muitos modelos probabilísticos de segurança não contemplam todos os possíveis tipos de falha (Choi et al., 2012). Outra dificuldade apontada é a falta de regulamentação específica para esse tipo de aplicação (IAEA, 2012).

Verificação e validação independentes

Um sistema digital de I&C deve atender aos requisitos de segurança licenciados durante todos os

Revista Teccen. 2019 Jan/Jun.; 12 (1): 50-59

Tabela 1. Requisitos para sistema I&C descritos no Guia SSR 2/1 da IAEA.

Número do requisito	Grupo	Descrição
59	Fornecimento de instrumentação	A I & C deve ser fornecida para: determinar os valores de todas as principais variáveis que podem afetar o processo de fissão, integridade do núcleo do reator, sistema de refrigeração do reator e contenção da usina; para obter informações essenciais sobre a planta, que são necessárias para uma operação segura e confiável; para determinar o estado da planta em condições de acidente; tomada de decisões em caso de acidente.
60	Sistemas de controle	Devem ser fornecidos sistemas de controle apropriados e confiáveis na usina para manter e limitar as variáveis de processo relevantes dentro dos intervalos operacionais especificados.
61	Sistema de proteção	Um sistema de proteção deve ser disponibilizado para a usina com capacidade de detectar condições inseguras e iniciar ações de segurança automaticamente para atuar sobre os sistemas de segurança necessários para alcançar e manter a planta em condições seguras.
62	Confiabilidade e testes dos sistemas de I & C	Sistemas de I & C para itens importantes para a segurança devem ser projetados com alta confiabilidade e testados periodicamente para atender à função de segurança executada.
63	Sistema importante para a segurança com equipamentos baseados em computadores	Se um sistema importante para a segurança da usina nuclear depender de equipamentos baseados em computadores, devem ser estabelecidos e implantados padrões e práticas adequadas para o desenvolvimento e teste de hardware e software durante toda a vida útil do sistema e, em particular, durante o ciclo de desenvolvimento do software. Todas as etapas do desenvolvimento devem estar sujeitas a um sistema de gestão da qualidade.
64	Separação entre os sistemas de controle e proteção	A interferência entre sistemas de proteção e controle da usina nuclear deve ser prevenida através de separação, evitando interconexões ou provendo uma independência funcional.
65	Sala de Controle	Uma sala de controle deve estar disponível em uma usina nuclear a partir da qual pode ser operada de forma segura em todos os estados operacionais, de forma automática ou manual e, a partir da qual possam ser tomadas medidas para se manter uma condição segura da planta ou para trazê-la a um estado seguro após condições operacionais antecipadas ou acidentes.
66	Sala de controle suplementar	Equipamentos de I & C devem estar disponíveis, de preferência em um único local (sala de controle suplementar): física, elétrica e funcionalmente separados da sala de controle principal da usina. A sala de controle suplementar deve estar equipada para que o reator possa ser levado e mantido desligado, removendo o calor residual e monitorando as variáveis essenciais da planta se ocorrer a perda das funções de segurança na sala de controle principal.
67	Instalações de resposta a emergência no sítio	A usina deve dispor de instalações de reposta a emergências no sítio. O projeto deve permitir que as equipes possam realizar tarefas para gerenciamento de emergências em condições de acidentes.

seus ciclos de vida e, por isso, deve seguir processos criteriosos de desenvolvimento e implantação (Kubde & Sable, 2014; Tommila & Alanen, 2015). Um processo de desenvolvimento empregado para o desenvolvimento de sistemas digitais é o de verificação e validação independentes (IV&V), onde porções pequenas de hardware e software são avaliadas até que se contemple toda a arquitetura projetada.

Os principais desafios para a implementação do IV&V são: garantir que a qualidade do desenvolvimento não será afetada por questões relacionadas a custo e prazos; controlar informações proprietárias ou no caso de contratação de empresas externas; disponibilizar de equipe de suporte (IAEA, 2012).

Gerenciamento da especificação de requisitos funcionais

A etapa de especificação dos requisitos funcionais dos sistemas de I&C determinará o sucesso da elaboração de um projeto. Uma falha na especificação pode reduzir a confiabilidade, ameaçar a segurança ou atrasar os processos de licenciamento e desenvolvimento da arquitetura necessária. Requisitos adequados devem atender a critérios de adequação, testes, verificação e rastreabilidade (IAEA, 2012).

Os principais desafios relacionados a especificação dos requisitos funcionais são: falta de orientações específicas para preparação de requisitos a nível de sistema; funcionalidades diferentes dos sistemas analógicos testados; necessidade de integração de diversas equipes com diferentes competências (IAEA, 2012).

Gerenciamento de configuração

O gerenciamento de configuração é um importante processo na caracterização de estruturas, sistemas e componentes (*SSC – Structures, Systems and Components*) de um reator nuclear. Esse processo é responsável por manter informações atualizadas sobre projeto, condições operacionais e modificações do projeto original da planta (IAEA, 2003). Para os sistemas digitais, esse processo torna-se ainda mais importante visto que é necessário um controle sobre a versão de software instalada em uma determinada etapa do ciclo de vida da usina (Chou, Hsiao & Chang, 2010).

O desafio do gerenciamento de configuração é garantir que os itens instalados estejam devidamente avaliados e qualificados conforme os requisitos reguladores (IAEA, 2012).

Falha de causa comum, diversidade e defesa em profundidade

Devido ao risco associado às radiações ionizantes, os projetos de usinas nucleares consideram vários níveis de barreias para evitar ou mitigar efeitos indesejáveis. O conceito de barreiras conhecido como defesa em profundidade considera diversos fatores relacionados a margens de projeto e disponibilidade de sistemas sob diversas situações e configurações. Para isso, os projetos consideram a possibilidade de existir equipamentos com mesma função que possam operar sob diversas configurações, definindo o conceito de redundância. Para que o efeito desejado seja alcançado, o conceito de diversidade física ou lógica visa garantir que a falha de um equipamento não interfira na operação de outro, caracterizando a diversidade. Mesmo com essas medidas de proteção, podem ocorrer falhas que podem ou não ter a mesma causa. Uma falha que afetar equipamentos de diferentes redundâncias é chamada de Falha de Causa Comum (*CCF – Common Cause Failure*) [6]. Em sistemas digitais de I&C, a caracterização da CCF dos variados softwares empregados apresenta-se como um fator crítico, devido à complexidade de se modelar e representar alguns modos de falha (IAEA, 2012). Adicionalmente, o controle das principais variáveis de processo pode sofrer influências indesejáveis em função de uma CCF.

Os desafios relacionados a falha de causa comum precisam considerar a necessidade de aplicação e validação de requisitos através de metodologias de análise dinâmica, e a disponibilização de sistemas de segurança alternativos de menor complexidade ou arquiteturas diferentes (IAEA, 2012). Sobre as metodologias de análise dinâmica, muitos estudos têm demonstrado a importância de cada técnica na análise de determinada característica, mas a maioria dessas pesquisas ressalta a importância de estudos mais abrangentes nessa área (U.S.NRC, 2006).

Uso de dispositivos inteligentes

A aplicação de dispositivos inteligentes em projetos de usina nuclear contempla a substituição de sensores e atuadores por dispositivos configuráveis com funções que possibilitem vários tipos de aplicações. Entretanto, a introdução desse tipo de dispositivo tem enfrentado resistência devido às dificuldades encontradas nos processos de qualificação, uma vez que algumas informações são de propriedade dos fabricantes e, por questões comerciais, tem acesso restrito. Além disso, esses dispositivos podem conter funções que não são usadas, mas que podem interferir nas ações requisitadas (IAEA, 2012).

Classificação de funções, sistemas e equipamentos em função dos requisitos de segurança

A classificação de estruturas, sistemas e componentes de uma usina nuclear deve atender aos requisitos vigentes no local de construção de uma usina. Entretanto, cada país tem cultura e requisitos próprios para classificar os sistemas de I&C em função dos seus parâmetros de segurança (WNA, 2015). Em alguns casos, alguns sistemas podem ser classificados de forma diferente em cada nacionalidade. Por outro lado, quando um projetista desenvolve um projeto, geralmente, leva em consideração os requisitos do seu país e contempla recomendações da IAEA. Quando um projeto é adquirido de um país com diferentes critérios

para classificação do grau de segurança de um sistema, questionamentos reguladores podem demandar pela inclusão de novos requisitos ou até mesmo a modificação de itens do projeto.

Um exemplo clássico dos problemas relacionados a diferentes classificações e solicitações de modificações do projeto original foram observados na construção da usina finlandesa de Olkiluoto 3 (WNA, 2015; Sandberg & Tiippana, 2005; Laaksonen, 2010). A construção da usina foi iniciada em 2005, com operação comercial inicialmente prevista para o ano de 2009, mas devido a vários problemas identificados a nova previsão é para o final do ano de 2018 (Laaksonen, 2010).

Segurança cibernética

Os ataques cibernéticos têm crescido em diversas áreas de atuação e tem se apresentado como grande fator de preocupação para se garantir disponibilidade, integridade, confidencialidade e autenticidade dos dados que trafegam pelas diferentes tecnologias de rede (Canongia & Junior, 2009; Dion, Howlader & Ewing, 2010; Shin, Son & Heo, 2013).

As dificuldades relacionadas à segurança cibernética estão relacionadas aos efeitos que uma intrusão maliciosa pode provocar na operação da usina ou em sistemas de segurança, pois a todo instante estão em desenvolvimento novas tentativas de invasão. Por motivos de segurança, as medidas de proteção precisam ser confidenciais, fato esse que limita a possibilidade de estudos de simulação e avaliação de possíveis comportamentos (IAEA, 2012).

Um caso famoso de invasão cibernética na área nuclear foi a descoberta de um sofisticado malware, batizado de Stuxnet, na instalação de enriquecimento de urânio iraniana de Natanz em 2010. Estudos mostram que o Stuxnet foi um ato de sabotagem, inserido via porta USB, que tinha por objetivo danificar centrífugas a partir do conhecimento de suas vulnerabilidades (Baezner & Robin, 2017).

Padronização de normas e guias reguladores

Cada país tem a soberania para definir suas normas, entretanto, a falta de padronização pode impedir a aplicação de determinada técnica ou produto em um processo globalizado (WNA, 2011). Por conseguinte, diversos institutos internacionais vêm desenvolvendo padrões mínimos cuja aplicação não irá se sobrepor a regulamentos específicos. Esses padrões visam facilitar a aceitação de projetos em diferentes culturas de licenciamento (IAEA, 2012).

A filosofia de harmonização de normas e padrões busca auxiliar os operadores e projetistas na especificação de equipamentos e, pelo aspecto regulador, almeja determinar a adequação dos projetos a parâmetros de segurança em concordância com os níveis de risco permitidos (WNA, 2011). Portanto, para se atingir o objetivo da harmonização, estudos devem levar em consideração a definição de um conjunto mínimo de padrões que possam ser usados em diferentes culturas de regulação (IAEA, 2012).

Monitoração em tempo real

A I&C de uma usina nuclear é composta por vários sensores que precisam ser periodicamente testados e calibrados que podem causar perda econômica, riscos e exposição à radiação dos trabalhadores (Labbe et al., 2012). Assim sendo, muitos estudos estão em execução para se comprovar os efeitos que processos de monitoração em tempo real (*OLM – online monitoring*) podem agregar à operação das plantas.

A dificuldade encontrada para a difusão do OLM é a falta de critérios de aceitação aprovados por reguladores que permitam a utilização de canais de instrumentação para calibração e testes de instrumentos (IAEA, 2012).

Qualificação de sistemas de segurança

Os equipamentos de segurança em um projeto de reator nuclear precisam desempenhar suas funções atendendo a todos os requisitos reguladores, em todo período de vida licenciada. Esse processo de qualificação considera a operação em condições normais ou para os acidentes postulados (IAEA, 1998). As primeiras recomendações para a qualificação dos equipamentos consideravam as condições ambientais onde os mesmos operavam (temperatura, radiação, umidade, etc.) e os riscos sísmicos. A introdução de sistemas digitais evidenciou a necessidade de se qualificar os equipamentos de I&C em função de interferências provenientes de fontes eletromagnéticas (*EMI – Electromagnetic Interference*) e de radiofrequência (*RFI – Radio Frequency Interference*) (IAEA, 2012).

Apesar de terem objetivos diferentes, diversos organismos internacionais têm aprimorado seus processos de qualificação de equipamentos e a convergência dos mesmos é um obstáculo que ainda deve ser vencido (IAEA, 2012).

Impacto da linguagem de configuração de hardware em dispositivos programáveis

Devido aos problemas relacionados ao licenciamento de software, muitos projetos de sistemas digitais de I&C têm considerado a aplicação de

dispositivos programáveis por linguagem de hardware (*HDL – Hardware Description Language*). Uma família de componentes que tem sido utilizada nos projetos e utilizam a linguagem HDL são os FPGA's (*Field Programmable Gate Array*) (Farias et al., 2016; Maerani, Mayaka & Jung, 2018). Alguns pontos ainda precisam ser avaliados para introdução desses dispositivos em sistemas de usinas nucleares como: banco de dados de confiabilidade, experiência operacional, definição de requisitos, adoção das funcionalidades já testadas, existência de um número reduzido de fornecedores qualificados para a área nuclear, dificuldades relacionadas à aplicação de métodos de codificação e desenvolvimento de ferramentas para validação (IAEA, 2012).

Comunicação digital

A integridade de dados digitais em qualquer meio de comunicação depende de diversos fatores relacionados às características do meio ou comportamento dos componentes empregados no projeto. Desse modo, a introdução de técnicas de modulação, codificação, protocolos e correção de erros tornam-se cada vez mais necessárias para se garantir a integridade da informação (Guimarães & Souza, 2012). Em um projeto de I&C digital a integridade da informação está diretamente relacionada a segurança da planta nuclear, uma vez que a recepção ou interpretação incorreta dos dados recebidos pode provocar uma atuação incorreta dos sistemas de segurança, podendo causar eventos iniciadores de situações de emergência (IAEA, 2012).

Em um projeto de I&C digital pode-se identificar três importantes tópicos que devem ser analisados: a comunicação entre diferentes sistemas, onde cada um pode ser enquadrado em diferentes classificações quanto à segurança; nível de prioridades, definindo qual sistema deve atuar inicialmente sobre a atuação em algum dispositivo do processo; apresentação de dados aos operadores, que permitirá a observação dos parâmetros operacionais e ações de acordo com os procedimentos de operação (IAEA, 2012).

A falta de estudos acerca do impacto da confiabilidade dos dados e do limite de erro aceitável para manutenção das condições de segurança apresentam-se como o maior desafio a ser enfrentado para a definição de requisitos sobre o tema.

Classificação quanto a segurança e função de controladores compactos

Muitos projetos de I&C consideram o emprego de controladores compactos, principalmente em funções de desligamento de emergência. Esses sistemas têm complexidade limitada para reduzir a possibilidade de falhas (Chung & Kim, 2003). A classificação desses tipos de controladores precisa ser profundamente estudada devido as consequências que uma falha pode provocar, entretanto, essa funcionalidade é de difícil avaliação devido a interação com outros níveis de automação (IAEA, 2012).

Métodos para desenvolvimento de Software

Os requisitos que norteiam a introdução de sistemas digitais de I&C na área nuclear demandam por processos formais de desenvolvimento de software (IAEA, 2012). Logo, uma sequência bem estabelecida e documentada deve ser considerada nas diversas fases do desenvolvimento do software, desde a sua concepção até o fim do ciclo de vida dos mesmos (Vital & Vital, 2015). Portanto, torna-se necessário o emprego de técnicas capazes de validar as características dos projetos que atendam aos requisitos regulatórios (IAEA, 2012).

Alguns setores econômicos trabalham com um nível tolerado de falhas em código, que não são aceitáveis na área nuclear. Esse dilema é um dos grandes desafios encontrados, visto que muitos métodos comerciais não possuem fácil aceitação na área nuclear. Adicionalmente, os recursos humanos disponíveis na área nuclear para o aperfeiçoamento de métodos formais de desenvolvimento de software são limitados (IAEA, 2012).

Utilização de tecnologias sem fio

As redes sem fio têm sido empregadas em diferentes ramos industriais, devido à possibilidade de comunicação a elevadas taxas de transmissão de dados e baixos custos de instalação e manutenção (IAEA, 2012) (Laaksonen, 2010). Nas usinas nucleares em operação essa implantação tem encontrado resistência, pois muitas usinas foram construídas antes do advento das modernas tecnologias de comunicação sem fio, limitando-se sua aplicação apenas a equipamentos que não sejam de segurança (Laaksonen, 2010). Essa demora decorre da falta de testes dos equipamentos instalados nas usinas sob operação conjunta com outros equipamentos de redes (Lowe et al., 2017). Os principais questionamentos desta aplicação estão relacionados à comprovação da robustez dos sistemas a interferências EMI/RFI (Ye et al., 2015). Os mecanismos de troca de experiência operacional mostram que alguns eventos observados em usinas nucleares foram atribuídos à operação de sistemas de comunicação sem fio (Ko & Lee, 2013).

Os principais desafios encontrados para o emprego das redes sem fio nas usinas nucleares residem na necessidade de se comprovar que as tecnologias

wireless podem operar sem comprometer a segurança destas e, ainda, na falta de regulamentação específica para esse tipo de comunicação em alguns países (IAEA, 2012).

Confiabilidade

A implantação de sistemas digitais de I&C nas usinas nucleares tem passado por grandes transformações e questionamentos, visto que uma falha de hardware ou software pode colocar a planta em uma condição insegura (Holmberg, Porthin & Tyrväinen, 2016). Uma questão que merece atenção é o impacto que a confiabilidade dos sistemas digitais provoca nas análises de segurança. Atualmente, existe um consenso que as metodologias de análise estáticas não são suficientes para representar as características de sistemas digitais, por outro lado, ainda não existem resultados suficientes para se determinar a melhor metodologia de análise dinâmica (U.S.NRC, 2006). Além disso, as metodologias dinâmicas nas Análises Probabilísticas de Segurança (APS) ainda não foram empregadas na representação completa de sistemas digitais devido a suas peculiaridades, como por exemplo, a quantificação da confiabilidade de software (Authén & Holmberg, 2012). Portanto, a maior dificuldade para se modelar os sistemas digitais depende do desenvolvimento e da aplicação das diversas metodologias existentes e, bem como da avaliação das contribuições em função das características dos sistemas modelados (IAEA, 2012).

Considerações finais

As informações apresentadas nesse trabalho ressaltam a importância que o atendimento aos requisitos reguladores locais tem sobre a implantação de sistemas digitais de I&C, seja na modernização de sistemas obsoletos ou no projeto de uma nova concepção de reator nuclear. Entretanto, verifica-se que ainda existem muitos desafios para a massificação dos sistemas digitais na configuração de usinas nucleares. Esses desafios têm provocado atrasos e elevação de custos na construção de novas gerações de reatores ou nos processos de modernização.

Devido à complexidade do processo de licenciamento dos sistemas digitais de I&C, aplicações com diferentes metodologias de análise dinâmica são importantes para a validação dos requisitos de segurança. À vista disso, este trabalho recomenda que a análise de funções dos sistemas digitais de I&C considere a aplicação de técnicas empregadas em estudos recentes como: Árvore de Falhas Dinâmica (*DET – Dynamic Event Tree*), Metodologia de Fluxo Dinâmico (*DFM – Dynamic Flow Methodology*), Redes Bayesianas, Redes de Petri, Mapeamento Célula a Célula (CCMT – Cell to cell mapping Technique), dentre outras.

Referências

Authén, S., Holmberg, J. E. (2012). Reliability analysis odd digital systems in a Probabilistic Risk Analysis for nuclear power plants. Nuclear Engineering and Technology, 44(5), 471-482.

Baezner, M., Robin, P. (2017). Stuxnet. Center for Security Studies, Zurich.

Canongia, C., Junior, R. M. (2009). Segurança cibernética: o desafio da nova Sociedade da Informação. Revista Parcerias Estratégicas, 14(29), 21-46.

Choi, J. G. et al. (2012). Fault detection coverage quantification of automatic test functions of digital I&C system in NPPS. Nuclear Engineering and Technology, 44(4), 421-428.

Chou, I., Hsiao, H. H., Chang, C. (2010). Developing software configuration management system for Digital Instrumentation and Control(DI&C) system of Nuclear power Plant. Proceedings of the 18th International Conference on Nuclear Engineering (ICONE18).

Chung, H. Y., Kim, D. W. (2003). Design of advanced power reactor (APR1400) I&C system. IFAC Power Plants and Power Systems Control, p. 729-734.

CNEN (2002). Licenciamento de instalações nucleares – Norma CNEN NE 1.04.

Dion, J., Howlader, M. K., Ewing, P. D. (2010). Wireless network security in nuclear facilities. NPIC&HMIT 2010, Las Vegas, p. 567-578.

Farias, M. S., Martins, R. H. S., Teixeira, P. I. N., Carvalho, P. V. R. (2016). FPGA-Based I & C systems in nuclear plants. Chemical Engineering Transactions, 53, 283-288.

Guimarães, D. A., Souza, R. A. A. (2012). Transmissão digital: princípios e aplicações. São Paulo: Brasil: Editora Érica.

Holmberg, J. E., Porthin, M., Tyrväinen, T. (2016). Reliability analysis of digital I&C in nuclear power plants. Proceedings of Nuclear Science and Technology Symposium (NST2016).

IAEA (1998), Equipment qualification in operational Nuclear Power Plants.

IAEA (2003), Configuration management in nuclear power plants.

IAEA (2010). Licensing process for nuclear installations - Specific Safety Guide N. SSG-12.

IAEA (2011). Core knowledge on instrumentation and control systems in nuclear power plants – Technical Report N. NP-T-3.12.

IAEA (2012). Assessing and managing cable aging in nuclear power plants – Technical Report N. NP-T-3.6.

IAEA (2015). Technical challenges in the application and licensing of digital instrumentation and control systems in nuclear power plants – Technical Report N. NP-T-1.13.

IAEA (2016a). Design of instrumentation and control systems for nuclear power plants - Specific Safety Guide N. SSG-39.

IAEA (2016b). Safety of nuclear power plants: design - Specific Safety Requirements, N. SSR-2/1, Rev. 1.

IAEA (2016c). Safety of nuclear power plants: commissioning and operation - Specific Safety Requirements, N. SSR-2/2, Rev. 1.

Ko, D. Y., Lee, S. I. (2013). Applicable approach of the wireless technology for Korean nuclear power plants. Nuclear Engineering and Design, 265, 519-525.

Kubde, P., Sable, D. (2014). The role of verification and validations in system development life cycle. International Journal of Research in Advent Technology, 2(2).

Laaksonen, J. (2010). Lessons learned from Olkiluoto 3 Plant. STUK – Radiation and Nuclear Safety Authority.

Labbe, A., Abdul-Nour, G., Vaillancourt, R., Komljenovic, D. (2012). Implementation of an on-line monitoring system for transmitters in a CANDU nuclear power plant. Journal of Physics, 364.

Lowe, C. L., Kiger, C. J., Jackson, D. N., Young, D. M. (2017). Implementation of Wireless Technologies in Nuclear Power Plants' – Electromagnetic Environment using Cognitive Radio System. NPIC & HMIT 2017, San Francisco.

Maerani, R., Mayaka, J. K., Jung, J. C. (2018). Software verification process and methodology for development of FPGA-based engineered safety features system. Nuclear Engineering and Design, 330, 325-331.

Rojo, F. J. R., Roy, E., Kelly, S. (2012). Obsolescence Risk Assessment Process Best Practice. Journal of Physics, 364.

Sandberg, J., Tiippana, P. (2005). Regulatory aspects of Olkiluoto 3 Nuclear Power Plant.

Shin, J., Son, H., Heo, H. (2013). Cyber Security Risk Analysis Model Composed with Activity-quality and Architecture Model. International Conference on Computer, Network and Communication Engineering (ICCNCE 2013), 609-612.

Tommila, T., Alanen, J. (2015). Conceptual model for safety requirements specification and management in nuclear power plants. VTT Technology.

U.S.NRC (2006). Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments - NUREG CR-6901.

Vital, R. B. N., Vital, T. M. (2015). Utilização da modelagem UML em um sistema de gerenciamento de uma franquia do setor de alimentação. Revista Teccen, 8(2), 65-72.

Wahlström, B. (2007). Safety of nuclear power; the case for I&C and HF engineering. EHPG meeting of the OECD Halden Reactor Project.

Wahlström, B. (2015). Differences between analog and digital I&C. 9th. International Conference on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies, Charlotte, 2015.

WNA (2011). International Standardization of Nuclear Reactor Designs.

WNA (2015). Classification for I & C systems in nuclear power plants – Current status and difficulties.

Wyatt, R. D., Supler, R. W. (2017). Development of functional requirements specification for digital instrumentations and control systems upgrades used at nuclear power plants (NPPs). NPIC&HMIT 2017, San Francisco.

Ye, S. H et al. (2015). Verification of electromagnetic effects from wireless devices in operating Nuclear Power Plants. Nuclear Engineering and Technology, 47(6), 729-737.